CanIt-PRO User's Guide

for Version 8.0.7

Roaring Penguin Software Inc.

16 June 2011

Contents

1 Introduction **11**

1.1 Organization of this Manual 11

1.2 Definitions 12

2 The Simplified Interface **15**

3 The *My Filter* Page **17**

3.1 Setting Filter Aggressiveness 18

3.2 Sender Rules 18

3.3 The Trap 18

3.4 Online Documentation 18

4 The CanIt-PRO Spam Trap **21**

4.1 Viewing the Spam Trap 21

4.1.1 Message Summary Display 21

4.1.2 Sort Order 22

4.1.3 Message Body Display 22

4.1.4 Summary of Links 23

4.2 Message Disposition 23

4.2.1 Quick Spam Disposal 24

4.3 Incident Details 24

4.3.1 Basic Details 25

4.3.2 Address Information 26

4.3.3 History 26

4.3.4 Spam Analysis Report 26

4.4 Viewing Other Messages 27

4.5 Viewing Specific Incidents 27

4.6 Searching the Trap . . . 27
4.7 Closed Incidents . . . 29
4.8 Whois Queries . . . 29
4.8.1 Sending Abuse Complaints . . . 30

5 Blacklists, Whitelists and Rules 33
5.1 The Sender Action Table . . . 33
5.1.1 Holding Unlisted Senders . . . 35
5.2 The Domain Action Table . . . 35
5.2.1 Domain Matching Rules . . . 36
5.3 The Network Action Table . . . 36
5.4 Country Rules . . . 37
5.5 Bulk Blacklisting and Whitelisting . . . 38
5.6 MIME Types . . . 39
5.7 Filename Extensions . . . 40
5.7.1 Matching Entire File Names . . . 41
5.7.2 Matching All Attachments . . . 41
5.8 Custom Rules . . . 42
5.8.1 Fields . . . 42
5.8.2 Relations . . . 43
5.8.3 Score . . . 44
5.8.4 Expiry . . . 44
5.8.5 Creating and Deleting Custom Rules . . . 44
5.8.6 Header Matching . . . 44
5.8.7 Body Matching . . . 45
5.9 RBL Rules . . . 45
5.10 Mismatch Rules . . . 46
5.11 SPF Rules . . . 47
5.11.1 How SPF Queries Work . . . 48
5.11.2 Entering SPF Rules . . . 49
5.11.3 Vouch by Reference . . . 49
5.12 DKIM Rules . . . 50
5.12.1 Vouch by Reference . . . 51
5.13 Blacklisting Recipients . . . 51
5.14 Enumerating Valid Recipients . . . 52

5.15 Importing and Exporting Rules . . . 53
5.15.1 Exporting Rules . . . 53
5.15.2 Format of the Exported Rules . . . 54
5.15.3 Importing Rules . . . 56
5.16 Reviewing the Change History . . . 56

6 Preferences **59**
6.1 Preferences . . . 59
6.2 Changing Default Preferences . . . 62
6.3 Changing your Password . . . 62
6.4 Quick Links . . . 62

7 Reports **63**
7.1 Statistics . . . 63
7.1.1 Classification Reports . . . 64
7.2 Reports based on Trap Content . . . 65
7.3 Greylisting Report . . . 67
7.4 Load Report . . . 67

8 Streams **69**
8.1 Opting Out of Spam Scanning . . . 69
8.2 Stream Settings . . . 69
8.3 Notification of Pending Messages . . . 72
8.4 RSS Feeds . . . 74
8.5 Adding Alternate Addresses . . . 75
8.6 Switching Streams . . . 76
8.6.1 Viewing All Streams at Once . . . 76

9 Bayesian Filtering **77**
9.1 Introduction to Bayesian Filtering . . . 77
9.2 Stream Settings Associated with Bayesian Filtering . . . 77
9.3 Training the Bayesian Filter . . . 79
9.3.1 Manual Voting . . . 80
9.4 Bayesian Score Settings . . . 80

10 Email Archiving **83**
10.1 Introduction to Archiving . . . 83

10.2 Configuring Archiving . . . 83
10.3 Archiving Outbound Mail . . . 84
10.4 Archiving Internal Mail . . . 84
10.5 Searching the Archives . . . 85
10.5.1 Fields . . . 86
10.5.2 Relations . . . 87
10.5.3 Creating a Query Expression . . . 87
10.5.4 Creating a Query Group . . . 88
10.5.5 Performing a Search . . . 88
10.5.6 Query Cookbook . . . 88
10.6 Saved Searches . . . 90
10.7 Viewing Archived Messages . . . 90
10.7.1 Redelivering Archived Messages . . . 91
10.8 Searching for Related Messages . . . 91
10.9 Seeing Access History . . . 91
10.10 Seeing Search History . . . 92

11 Locked Addresses **93**
11.1 Introduction to Locked Addresses . . . 93
11.2 How Locked Addresses Work . . . 93
11.3 Creating a Locked Address . . . 94
11.4 Viewing Locked Addresses . . . 95
11.5 Editing a Locked Address . . . 96
11.6 Deciding on a Lock Type and Violation Action . . . 97

12 Tips **99**
12.1 Don't Trust Sender Addresses . . . 99
12.2 Don't Trust Sender Domains . . . 99
12.3 You May Trust Relay Hosts . . . 99
12.4 Custom Rules . . . 100
12.4.1 General Recommendations . . . 100
12.4.2 Things to avoid . . . 100
12.5 Group High-Scoring Messages Together . . . 100
12.6 Roaring Penguin Best-Practices . . . 101
12.7 General Anti-Spam Tips . . . 101
12.7.1 Use Receive-Only Addresses on your Web Site . . . 101

12.7.2 Do Not Reply to Spam . . . 101

A Mail headers added by CanIt-PRO **103**

A.1 General Headers . . . 103

A.1.1 X-Spam-Score . . . 103

A.1.2 X-CanItPRO-Stream . . . 105

A.1.3 Subject . . . 105

A.1.4 X-Spam-Flag . . . 105

A.1.5 X-CanIt-ID . . . 105

A.2 Bayesian Filtering Headers . . . 106

A.2.1 X-Bayes-Prob . . . 106

A.2.2 X-Canit-Stats-ID . . . 106

A.2.3 X-Antispam-Training-(Spam,Nonspam,Forget) . . . 106

A.3 Geolocation Header . . . 107

B The CanIt-PRO License **109**

B.1 THE CANIT DATA LICENSE . . . 112

Index **113**

List of Figures

2.1 Simplified Interface 15

3.1 My Filter 17

4.1 Pending Messages 21
4.2 Checkboxes 24
4.3 Incident Page 25
4.4 Trap Search 28
4.5 Whois Query 30
4.6 Spam Complaint 31

5.1 Sender Action Table 33
5.2 Domain Action Table 35
5.3 Network Action Table 37
5.4 Country-Code Rules 38
5.5 Bulk Entry 39
5.6 MIME Types 40
5.7 Filename Extensions 41
5.8 Custom Rules 42
5.9 RBL Rules 45
5.10 Mismatch Rules 46
5.11 SPF Rules 48
5.12 DKIM Rules 50
5.13 Export Rules 53
5.14 Import Rules 56
5.15 Change History 56

6.1 Preferences 60

7.1 Statistics 63
7.2 Virus Statistics 65
7.3 Sender Report 66
7.4 Cluster Load 67

8.1 Stream Settings 70
8.2 Notification Page 73
8.3 RSS Feed Page 74
8.4 Example Feed Reader 75
8.5 Set Default Stream 76

9.1 Bayes Voting Screen 79
9.2 Bayes Settings 81

10.1 Archive Configuration Screen 83
10.2 Archive Search Page 85
10.3 Saved Archive Searches 90
10.4 Archive Redelivery Page 91

11.1 Locked Address Creation 94
11.2 New Locked Address 95
11.3 Locked Address Listing 95
11.4 Locked Address Editor 96

Chapter 1

Introduction

Unsolicited commercial e-mail (UCE), or *spam*[1], is a pervasive problem. More and more unwanted messages are clogging mail servers and wasting employees' time. CanIt-PRO is a piece of software that runs on your mail server, scanning e-mail messages and picking out those which it considers to be spam. Messages identified as spam are held until a human examines them, and marks them as definite spam, in which case they are discarded, or as legitimate messages, in which case delivery is permitted.

1.1 Organization of this Manual

This manual is divided as follows:

Chapter 1, "Introduction", is this chapter. You should familiarize yourself with the terms in Section 1.2 before proceeding.

Chapter 2, "The Simplified Interface", describes the CanIt-PRO simplified interface for beginning users.

Chapter 3, "The *My Filter* Page", describes CanIt-PRO home page that lets you see the status of your filter at a glance.

Chapter 4, "The CanIt-PRO Spam Trap", describes CanIt-PRO's quarantine area and how to use it.

Chapter 5, "Blacklists, Whitelists and Rules", explains how you can create additional rules for blocking or accepting e-mail.

Chapter 6, "Preferences", explains how to set your personal CanIt-PRO preferences.

Chapter 7, "Reports", explains the types of reports CanIt-PRO can produce.

Chapter 8, "Streams", describes the concepts behind a *stream*. CanIt-PRO puts all of your e-mail, rules and settings into a stream.

Chapter 9, "Bayesian Filtering", explains CanIt-PRO's Bayesian filtering module. Bayesian filtering uses statistical analysis and training so that CanIt-PRO "learns" to recognize spam based on user feedback.

Chapter 11, "Locked Addresses", describes how CanIt-PRO permits users to generate addresses that

[1] SPAM is trademark of Hormel Foods Corporation, which graciously permits the term *spam* to be used to denote UCE

they can give out to strangers, but that those strangers cannot in turn give or sell to third-parties.

Chapter 12, "Tips", contains guidelines for reducing your workload and for dealing with spam more effectively.

1.2 Definitions

We use many terms related to Internet e-mail in this manual. Here is a definition of some of the terms we use.

Backscatter Unwanted DSNs (see "DSN") caused when e-mail systems respond to faked sender addresses.

Bayesian Analysis is a method whereby an anti-spam system keeps track of how often words appear in spam and non-spam. Once enough statistics have been accumulated, the system can calculate the likelihood that a new message is spam.

Blacklist A list of domains, senders or hosts that are blocked from sending e-mail.

CIDR "Classless Inter-Domain Routing". A method for specifying an entire set of contiguous IP addresses.

CanIt-Domain-PRO is an enhanced version of CanIt-PRO that allows two levels of delegation of responsibility. See the next three definitions for more details.

CanIt-PRO is an enhanced version of CanIt that allows flexible delegation of spam-control responsibilities rather than requiring a single spam-control officer.

CanIt is extra software built on top of MIMEDefang that provides sophisticated spam-management functions.

Cron A UNIX program that runs tasks periodically.

DNS "Domain Name System". The mechanism used on the Internet to translate host names to IP addresses and more generally, to associate various sorts of information with domain names.

DSN "Delivery Status Notification". A message generated automatically to notify senders of problems or failure to deliver an e-mail.

Daemon A long-running UNIX program that typically starts at system boot and continues running in the background until the system is shut down.

Envelope Mail messages often have *headers* specifying the sender (the "From:" header) and recipients (typically the "To:" header.) However, SMTP has a completely separate set of commands for specifying the sender and recipients. The sender and recipients specified in the SMTP commands are referred to as the *envelope sender* and *envelope recipients*, and do not necessarily match the information in the message headers. CanIt-PRO uses both the Header From and Envelope Sender address in Sender and Domain rules. It always uses only Envelope Recipients in its recipient rules.

Envelope Sender The sender address used in the "MAIL FROM" SMTP command. This is not necessarily the same as the *Header From* address. Most email readers display the Header From address rather than the Envelope Sender address.

Hash An algorithm that computes a short "signature" given a chunk of data. Different inputs are very likely to yield different signatures, so that a signature can be considered as a short-hand identifier for the original data.

Header From The sender address used in the "From:" header of an email message. This is the sender address displayed by most mail readers. See *Envelope Sender* for information about the SMTP sender address.

Greylisting A technique to block spam from certain spam-sending software. It works by issuing a Temporary Failure Code the first time an e-mail arrives from an unknown sender and IP address. Legitimate SMTP servers will retry, allowing the message to be delivered. Some spam-sending software does not retry, and messages sent by such software will be blocked without any content-scanning if greylisting is enabled.

Joe-Job A technique in which spammers fake the sending address to be that of an innocent victim, who often receives DSNs (see "DSN") and complaints.

MIMEDefang is a free (GPL'd) e-mail scanning program that integrates with Sendmail's Milter API. It forms the basis for CanIt.

MIME "Multipurpose Internet Mail Extensions". A set of rules for encoding different types of attachments as plain-text messages for transmission over SMTP.

Milter is a Sendmail interface that allows external programs to listen in on the SMTP dialog, and potentially modify Sendmail's actions and SMTP responses.

Mismatch Rule A rule that restricts which hosts are allowed to send mail on behalf of a particular domain.

Permanent Failure Code Also called **reject**, this is a code sent to a relay host telling it that e-mail transmission has failed and will not succeed. (For example, this code is sent if someone tries to send e-mail to a nonexistent user.) The relay host typically e-mails a failure notification to the original sender and discards the message.

Phishing An attack in which someone forges e-mail pretending to be from a security organization, a bank, etc. and convinces naive users to reveal sensitive information like user-names and passwords.

PostgreSQL A free and open-source SQL database heavily used by CanIt-PRO.

RBL "Real-time Blocklist". A DNS-based system for checking in real-time whether or not hosts or domains should be blocked.

RPTN is the Roaring Penguin Traning Network. This is a system whereby multiple CanIt-PRO installations can share Bayes training data.

RSS stands for "Really Simple Syndication" and is a format for publishing "news feeds" on the Web. CanIt-PRO can produce an RSS feed showing pending incidents.

Relay Host When a mail server wishes to transmit e-mail to your server using SMTP, it establishes a connection with your mail server. The machine attempting to transmit mail to your server is called a **relay host**.

Root Privileges A CanIt-PRO user with root privileges can create other users and configure basic operating parameters. Also, he or she can edit other users' preferences and stream settings.

SMTP Dialog During the course of e-mail transmission, the two ends of an SMTP connection transmit commands and results back and forth. This conversation is called the **SMTP dialog**.

SMTP "Simple Mail Transfer Protocol", as described in Internet RFC 2821. This is the protocol used to transmit e-mail over the Internet.

SPF stands for "Sender Policy Framework". It is a mechanism that allows a domain's administrator to list which hosts are allowed to originate e-mail claiming to come from that domain. For more details, please see `http://www.openspf.org`.

Sender's Domain This is the domain part (everything after the `@` sign) in the sender's e-mail address.

Sendmail A UNIX-based program for sending and receiving e-mail. Sendmail is designed to route mail from one mail server to another.

Spam Score A numerical score computed by CanIt-PRO that rates the likelihood that a message is spam.

Stream is a "virtual CanIt" machine offered by CanIt-PRO. If an incoming e-mail arrives for more than one recipient, and the recipients each wish to have his or her own private spam trap, CanIt-PRO re-mails the original message so each recipient has his or her own copy, and can dispatch it as he or she sees fit.

Syslog A UNIX program that centralizes the logging of messages from various system daemons.

Tempfail See "Temporary Failure Code"

Temporary Failure Code Also called **tempfail**, this is a code sent to a relay host telling it that e-mail transmission has failed temporarily, and it should retry in a little while. Typically, the relay host retains the e-mail message in a spool directory and retries transmission periodically. The host eventually gives up after a certain period (typically, a few days) has elapsed without successful transmission.

Ticker A CanIt-PRO program that runs periodic maintenance tasks.

Whitelist A list of domains, senders or hosts whose e-mail is permitted through without spam-scanning.

Chapter 2

The Simplified Interface

CanIt-PRO is extremely versatile, allowing you to set many parameters such as blacklists, whitelists, custom rules, and so on. If you find this too confusing and time-consuming, you can make use of the Simplified Interface. (Note that your system administrator must have configured CanIt-PRO to support this; if the simple interface is not available, it could be that your system administrator decided not to turn it on.)

If you enable the Simplified Interface (by clicking on **Simplified Interface** in the main menu), the CanIt-PRO interface looks something like this:

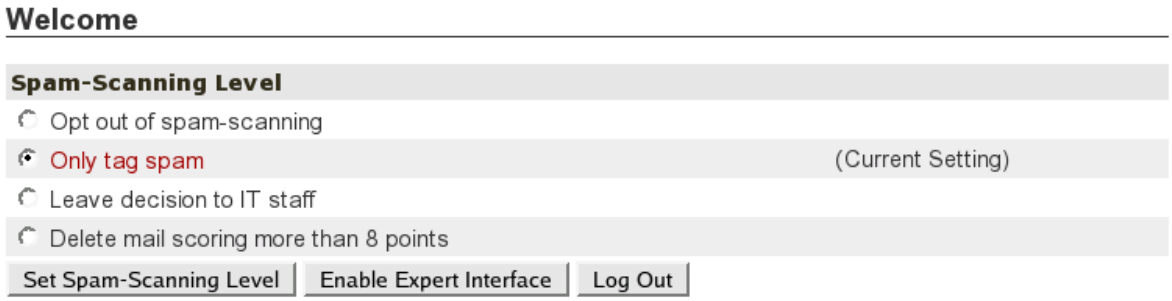


Figure 2.1: Simplified Interface

(Note that the specific choices might be different, depending on how your system administrator configured CanIt-PRO.)

To set a spam-scanning level, simply enable the appropriate button and click **Set Spam-Scanning Level**.

To log out, click on **Log Out**.

To turn on the normal interface, click **Enable Expert Interface**. The expert interface will be described in subsequent chapters.

Chapter 3

The *My Filter* Page

The home page in the Expert Interface is the “My Filter” page:

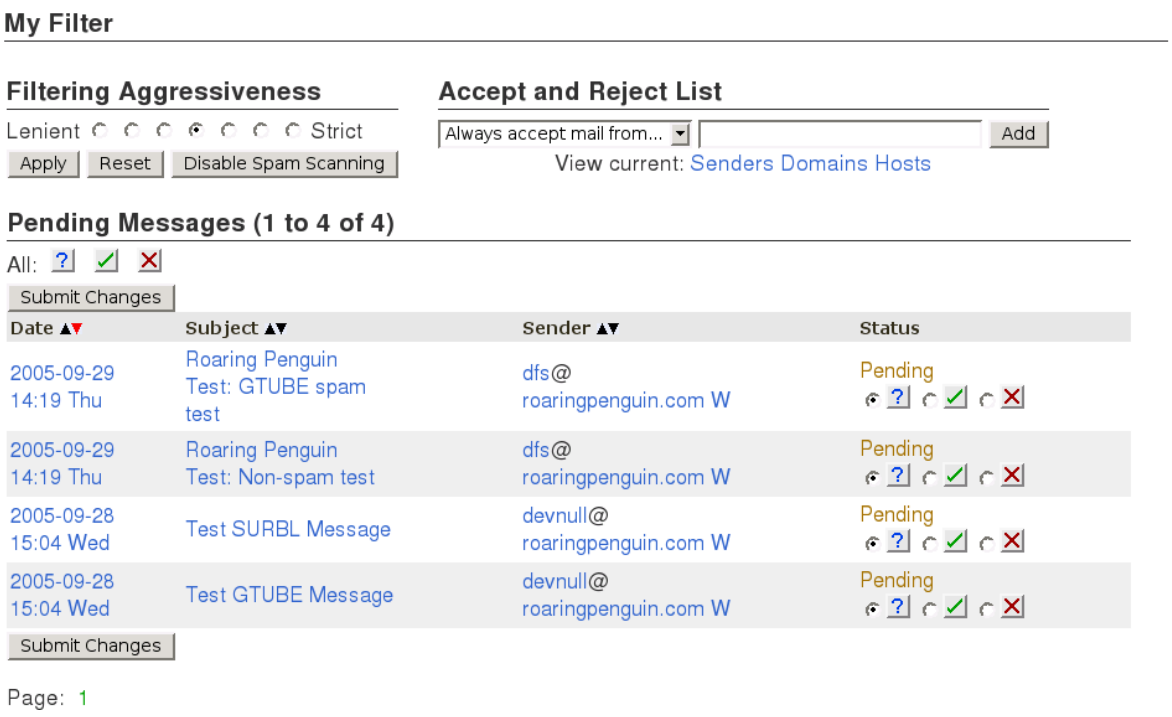


Figure 3.1: My Filter

The My Filter page is an overview of your filter settings and pending messages. Most of your interaction with CanIt-PRO can be done right on this page.

3.1 Setting Filter Aggressiveness

To set your filter's aggressiveness, click on one of the radio buttons from "Lenient" to "Strict". The strictest setting corresponds to holding all messages that score 3.5 or higher (scoring is explained in Chapter 4.) The most lenient setting corresponds to holding messages that score 6.5 or higher. The middle (and recommended) setting holds messages that score 5 or higher.

You can disable spam scanning completely by clicking **Disable Spam Scanning**. Click on **Enable Spam Scanning** (which appears only if spam-scanning is currently disabled) to re-enable spam-scanning.

3.2 Sender Rules

From the My Filter page, you can quickly add a sender address or domain, and tell CanIt-PRO always to accept mail from that address or domain. Simply set the pulldown menu to "Always accept mail from...", enter the address or domain in the text box, and click **Add**.

Conversely, you can tell CanIt-PRO to always reject mail from a sender or domain by changing the pulldown menu to "Always reject mail from...", entering the address or domain, and clicking **Add**.

Sender rules are more fully explained in Sections 5.1 and 5.2.

3.3 The Trap

Under the settings and sender rule areas, the My Filter page displays pending messages. These are messages that CanIt-PRO thinks might be spam. To release a message, click on the corresponding green checkmark. To reject a message, click on the red X. After you have chosen what to do with trapped messages, click **Submit Changes**. Messages you have chosen to reject will be discarded, while those you have chosen to accept will shortly be delivered to your mailbox. (This may take anywhere from a few minutes to a couple of hours, depending on how your administrator has configured CanIt-PRO.)

If you are not sure if a message is spam or not, click on the subject to see the first part of the message body. This usually provides sufficient context for you to make the decision.

If you click on the message date, CanIt-PRO will display a detailed analysis of why the message was held in the pending trap.

Click on the sender address (the part before the "@" sign) to add a rule pertaining to that sender. Click on the sender domain (the part after the "@" sign) to add a rule for that domain.

3.4 Online Documentation

This User's Guide (and depending on your privileges, other manuals) is available online in HTML format from the CanIt-PRO Web interface. The manuals may be accessed in a number of ways:

- Most pages have an "Online Documentation" link near the top right corner. This is a link to the section of the manual that describes that page.
- The bottom of each page includes a link to the User's Guide. If you have sufficient privileges, you will be given links to the API Guide, Administration Guide and Installation Guide as well.
- The bottom of each page includes a search box. To search the manuals, type a search phrase in the box and press enter. All manuals to which you have access will be searched and the search results presented. Note that the search is fairly simplistic: It just searches for a substring anywhere in the manual. When you click on a search hit, you may need to use the search function in your browser (typically, Control-F) to find the exact location of your search terms.

Chapter 4

The CanIt-PRO Spam Trap

The CanIt-PRO Spam Trap is a quarantine area in which CanIt-PRO holds messages that it thinks might be spam.

4.1 Viewing the Spam Trap

To view pending messages in the spam trap, click on the "Trap Contents" link. The pending messages screen will appear.

Figure 4.1: Pending Messages

4.1.1 Message Summary Display

The fields in the display have the following meanings:

Date is the date and time the message was first received.

Subject is the message subject.

Sender is the sender in the From: header of the message. If the Header From address does not match the Envelope Sender address, CanIt-PRO displays a warning like this: **(!)** If your mouse pointer hovers over the warning, CanIt-PRO displays the Envelope Sender address. Note that spammers can easily fake both the Header From and the Envelope Sender address.

Relay is the SMTP relay host which transmitted the message. This is somewhat harder to fake than the sender address. Note that sometimes a message can be sent from more than one SMTP relay host. If that is the case, you need to look up the incident details (described later) to get a list of all the relay hosts.

If CanIt-PRO can determine the country in which the sending relay is located, it displays a small country-flag to indicate the country of origin.

Score is the spam score assigned by the spam-scanning rules. The higher the score, the more "spam-like" the message appears. Any message scoring 5 or higher is held in the pending trap.

A message may be held even if it scores lower than 5. If this is the case, a "Hold Reason" will appear below the score. Possible hold reasons are:

HoldRelay You have asked CanIt-PRO to always hold messages from the sending relay.

HoldSender You have asked CanIt-PRO to always hold messages from the sender.

HoldDomain You have asked CanIt-PRO to always hold messages from the sender's domain.

HoldRBL The sending host is in a real-time blacklist, and you have asked CanIt-PRO to hold mail from hosts in the blacklist.

HoldVirus A virus was detected in the message, and you have asked CanIt-PRO to hold messages containing viruses.

HoldMIME The message was held because of a MIME type rule.

HoldEXT The message was held because of a filename extension rule.

Status and Action shows the current status of the message, and lets you determine the fate of pending messages. This will be described more fully in Section 4.2.

4.1.2 Sort Order

Normally, CanIt-PRO sorts messages in order of date received, with most recent messages first. You can click on the arrow near the "Score" column (for example) to sort by score. Click on the little up-arrow in a column to sort by that column in ascending order. Click on the down-arrow to sort in descending order. CanIt-PRO colors the little arrow corresponding to the current sort order red.

You can change the default sort order on your preferences page, described in Section 6.1.

4.1.3 Message Body Display

To view the body of a particular message, click on the message subject. The first 8kB of the message body will be displayed.

4.1.4 Summary of Links

The Message Summary Display contains many hyperlinks. These links are as follows:

- Click on the **Date** to display incident details (see Section 4.3.)
- Click on the **Subject** to display the first 8kB of the message body. Note that some spammers try to hide messages by encoding them using Base64 encoding (a special encoding for transmitting binary data.) Click on **Base64-Decoded Message** at the top of the message display to decode the message. You can also click on **Strip HTML Tags** to more easily read the text of HTML messages. (The **Base64-Decoded Message** link may not be available; it appears only if the administrator has configured CanIt-PRO to hold both raw and decoded messages.)
- The **Sender** entry is split over two lines. Click on the first line (`user@`) to open the Sender Action page (Section 5.1). Click on the second line (`domain.com`) to open the Domain Action page (Section 5.2). Finally, click on the "W" to perform a WHOIS query on the domain (Section 4.8 on page 29).
- The **Relay** entry is split over two lines. Click on the first line (the relay's IP address) to open the Network Action page (Section 5.3.) Click on the second line (the relay's host name, if resolvable) to open a WHOIS query on the relay's IP address.

4.2 Message Disposition

In the message summary display, any **pending** message has an entry box for controlling the disposition of the message. The possible values for the action are:

Do Nothing – leave the status of the message as **pending** for now.

Accept Message – mark the message as **not-spam** so it will be accepted the next time it is received.

Reject Message – mark the message as **spam** so it will be rejected.

Blacklist host – mark the message as **spam** and in addition, ban connections from the SMTP relay host (or hosts) which transmitted the message.

Whitelist host – mark the message as **not-spam** and in addition, do not hold any messages from the SMTP relay host (or hosts).

Blacklist sender – mark the message as **spam** and automatically reject any future messages from the sender.

Whitelist sender – mark the message as **not-spam** and automatically accept any future messages from the sender.

Blacklist domain – mark the message as **spam** and automatically reject any future messages from the domain. (The domain is everything after the `@` in the sender's address.)

Whitelist domain – mark the message as **not-spam** and automatically accept any future messages from the domain.

Silently discard – silently discard the message. Neither the sender nor the recipient will receive notification that the message was lost. *Do not use this option lightly; it is considered a serious breach of Internet etiquette to silently discard e-mail.*

To set message dispositions, set the action boxes appropriately and then click on **Submit Changes**. A summary of the actions will appear.

Note that if you set the **Method for choosing spam-trap actions** preference to "Checkbox" (Section 6.1 on page 59), then instead of a drop-down list, you get a series of buttons like this:

Figure 4.2: Checkboxes

- Select the red "X" to reject a message.
- Select the green check mark to accept a message.
- Select the question-mark to take no action.

4.2.1 Quick Spam Disposal

If your browser is JavaScript-enabled, then a line of buttons similar to Figure 4.2 appears after the word "All" near the top of the display. This lets you set all the action boxes on the page with one click:

- Select the question-mark to set all action boxes to **Do Nothing**.
- Select the red "X" to set all action boxes to **Reject message**.
- Select the green check mark to set all action boxes to **Accept message**.

4.3 Incident Details

To view the details about a pending-message incident, click on the date of the particular message. The incident page appears.

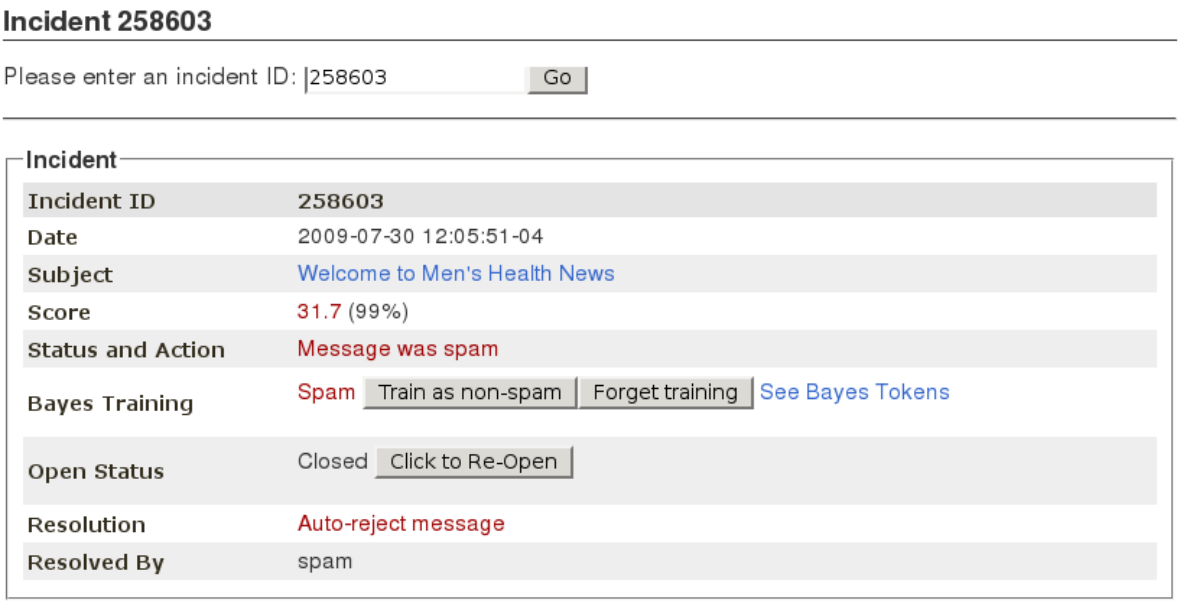


Figure 4.3: Incident Page

The Incident page contains the following information:

4.3.1 Basic Details

Incident ID is an integer assigned to each incident. This ID is sent in the SMTP failure messages so you can trace down a spam incident.

Date is the date the message was first received.

From is the Header From (the address in the From: header of the message.) If this is different from the Envelope Sender, a warning indicator appears. Hover over the indicator to see the Envelope Sender.

Subject is the message subject. Click on the subject to see the message body.

Decoded Subject is a decoded version of the message subject. Sometimes e-mail programs encode the subject, making it unreadable. If this is the case, CanIt-PRO will decode the subject and display it.

Score is the spam-scanning score.

Status and Action is the incident status. It is one of the following:

- New incident; only one transmission so far.
- This incident is still open.
- Message was not spam.

- Message was spam.

Bayes Training tells you how the incident was trained in the Bayes database, and give you an option to change the training. Note that this line will not appear if the Bayes signature has expired from the database (CanIt-PRO retains Bayes training information for only a short time, typically three days.)

Open Status tells you whether or not the incident is **open**. See Section 4.7 on page 29 for details.

Resolution is the action that was taken to dispose of the incident. If the incident is still pending, you will have an opportunity to dispose of it here.

Resolved By is the user who resolved the incident. The special system-user $\star$ is used for unresolved incidents, expired messages and automatically-rejected messages.

4.3.2 Address Information

The host information table is a table with a row for each relay host which attempted to deliver the message. The table contains the time the host first attempted delivery, the envelope sender, the relay host IP address and host name, and the number of delivery attempts from that host. Click on the relay IP to open the Network Action page for that relay, or on the relay name to perform a WHOIS query.

The recipients table lists all of the recipients of the message.

4.3.3 History

The history table is a log of actions taken for this incident. This logs when the incident was opened, and when it was closed (and who closed it.) The columns in the history table are as follows:

- **Who**: The user who performed the action. Actions performed by CanIt-PRO itself are marked with a user of $\star$.
- **When**: The date and time an action took place.
- **What**: A description of the action.
- **CanIt Host**: The host on which the action was performed. This column is likely of interest only to CanIt-PRO administrators.
- **Queue-ID**: The Sendmail Queue-ID associated with the action. Again, this column is likely of interest only to CanIt-PRO administrators.

4.3.4 Spam Analysis Report

Finally, the spam analysis report is a list of spam-scanning rules which triggered, along with the weight assigned to each rule.

4.4 Viewing Other Messages

In addition to pending messages, you can view other messages in the trap by following these links:

Pending shows messages whose status is **pending**.

Spam shows messages whose status is **spam**.

Non-Spam shows messages whose status is **not-spam**.

All shows all messages.

4.5 Viewing Specific Incidents

To view an incident given its incident ID, click on **Trap Contents** and then **Specific Incident**. Type the incident ID and press Enter.

You can view another incident by typing its ID in the box and pressing Enter.

If you enter an incident ID that you know exists, but CanIt-PRO cannot find it, the incident may not be in the current stream. If you are the CanIt-PRO administrator, switch to the stream "*" (a single asterisk) and re-enter the incident ID. This will search for the incident in all streams.

4.6 Searching the Trap

CanIt-PRO supports advanced queries on the spam trap. To open the Search page, click on **Trap Contents** and then **Search**. The Trap Search page appears:

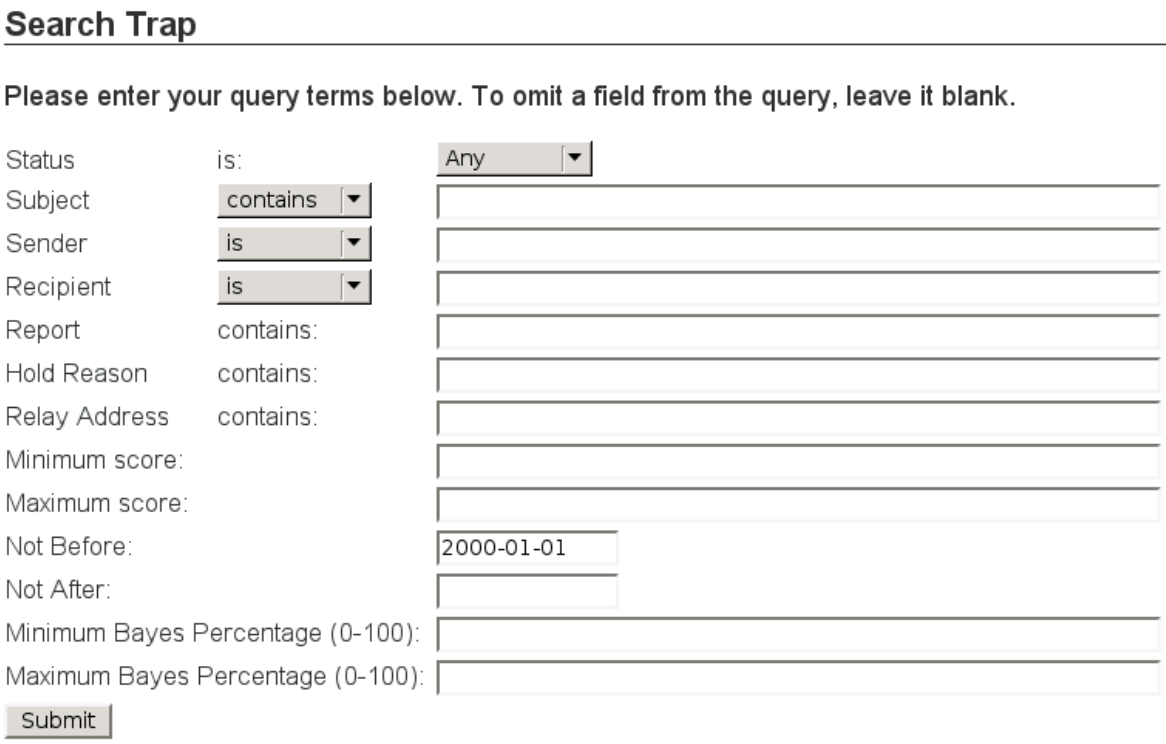


Figure 4.4: Trap Search

To perform a search:

- Set the **Status** field to one of "Any", "Pending", "Spam", or "Non-Spam", depending on how you want to restrict the query.
- Enter text in the **Subject** field to restrict the display to messages whose subjects contain that text. You can choose from **contains**, **is** or **starts with** to control how CanIt-PRO performs the search.
- Enter text in the **Sender** field to restrict the display to messages whose senders contain that text. Once again, you can choose from **contains**, **is** or **starts with**.
- Enter text in the **Recipient** field to restrict the display to messages whose recipients contain that text. You have the same three choices of match type as for Sender.
- Enter text in the **Report** field to restrict the display to messages whose spam reports contain that text. For example, you could enter "Custom rule" to match only messages that triggered a custom rule.
- Enter text in the **Hold Reason** field to match by hold reason. For example, you could enter "HoldMIME" to find messages that were held because of MIME-type matching rules.
- Enter minimum and/or maximum scores or Bayes percentages in the appropriate field to limit the search to incidents within the specified bounds.

- Select appropriate dates in the **Not Before** and **Not After** fields to restrict the search to a date range.
- Press **Submit Query** to run the query.

If you do not wish to restrict a query by a particular field, merely leave the corresponding entry box blank. Note that sender queries use both the Header From and Envelope Sender address. However, recipient queries use the SMTP recipients only, not the contents of the `To:` or `Cc:` e-mail headers. Also, sender and recipient queries may be slower than subject queries.

4.7 Closed Incidents

When an incident is first created as a pending incident, you can change the disposition of the incident. (For example, you can accept it, mark it as spam, whitelist the sender, etc.)

Some time after you dispose of an incident, it becomes **closed**. A closed incident is one whose disposition cannot be changed, because the message has already been handled by CanIt-PRO.

The rules for closing an incident are as follows:

- If the message was stored locally, then it is closed as soon as you either accept or reject the message. No further changes are possible.
- If the message was kept on the sending relay using temporary-failure codes, then the incident is closed on the first retransmission after you have marked the message for acceptance or rejection. Thus, there is a small (and unpredictable) window after you mark the message, but before it is retransmitted, during which you can change your mind.

Sometimes, it is desirable to reopen an incident. If you mistakenly rejected a message and would like the sender to re-send it, you *must* first mark the message as acceptable before asking the sender to re-send it. Otherwise, if it comes in again, CanIt-PRO will automatically reject it (because it has been marked as spam.)

To reopen an incident, open the incident page (Section 4.3) and click on **Click to Re-Open**. This will reopen the incident and let you change its disposition.

Note: Opening an incident won't automatically cause the message to be delivered if it was originally rejected in error. You'll have to make arrangements with the sender to send another copy.

4.8 Whois Queries

Clicking on the "W" or a host name in the Message Summary Display or Incident Details pages fires off a WHOIS query. These queries may help you discover who is responsible for spam relays, and may let you direct complaints appropriately.

Figure 4.5 illustrates a WHOIS query:

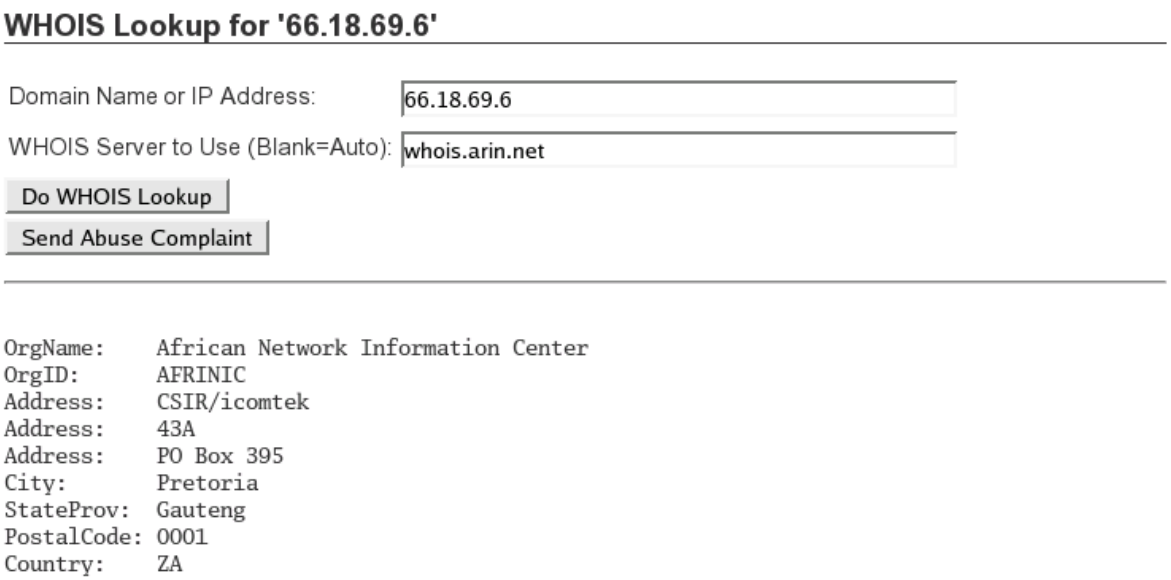


Figure 4.5: Whois Query

CanIt-PRO can handle WHOIS queries on domain names and IP addresses. In most cases, it can figure out the correct WHOIS server to use, and can handle referrals for the `.com`, `.net` and `.org` domains. However, you may have to help it out sometimes by supplying a WHOIS server name and clicking **Do Whois Lookup**.

CanIt-PRO performs simple-minded parsing of the WHOIS output:

- Any string beginning with `http://` is converted into a hyperlink.
- Any string with an `@` sign is converted to a `mailto:` hyperlink. You should be able to click on e-mail addresses to fire up your mail client.
- Any string in parentheses is assumed to be a "NIC Handle". Click on it to perform a WHOIS search on the handle. In the example, we see that NETBLK-CAIS-CIDR7 and CAIS-NOC-ARIN are correctly identified as NIC handles. Unfortunately, the (703) area code is incorrectly identified; you'll have to use your judgement.

4.8.1 Sending Abuse Complaints

If you opened a WHOIS search based on the IP address of an SMTP relay, there may be a button at the bottom of the WHOIS page that reads **Send abuse complaint**. This link is present *only if:*

- You clicked on the IP address of an SMTP relay.
- The IP address you clicked on is part of a CanIt-PRO incident.

If you click on the **Send Abuse Complaint** button, the Spam Complaint page appears (Figure 4.6).

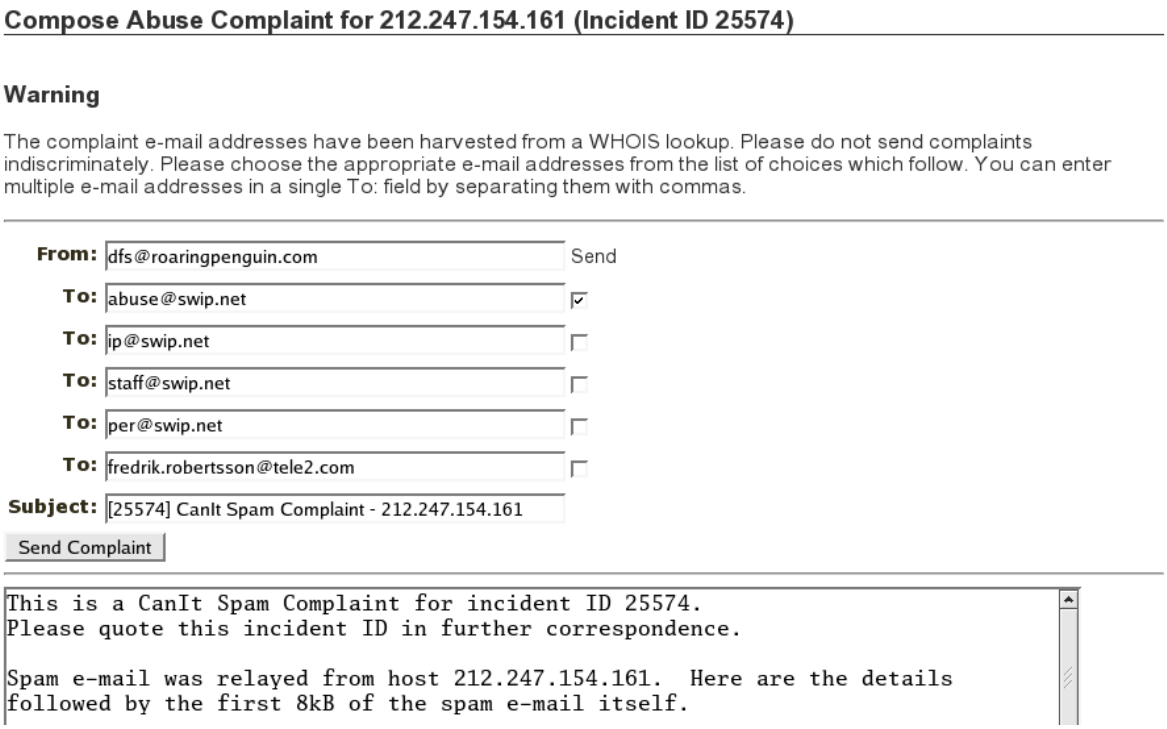

Compose Abuse Complaint for 212.247.154.161 (Incident ID 25574)
Warning
The complaint e-mail addresses have been harvested from a WHOIS lookup. Please do not send complaints indiscriminately. Please choose the appropriate e-mail addresses from the list of choices which follow. You can enter multiple e-mail addresses in a single To: field by separating them with commas.
From: dfs@roaringpenguin.com Send
To: abuse@swip.net
To: ip@swip.net
To: staff@swip.net
To: per@swip.net
To: fredrik.robertsson@tele2.com
Subject: [25574] CanIt Spam Complaint - 212.247.154.161
Send Complaint
This is a CanIt Spam Complaint for incident ID 25574.
Please quote this incident ID in further correspondence.
Spam e-mail was relayed from host 212.247.154.161. Here are the details
followed by the first 8kB of the spam e-mail itself.

Figure 4.6: Spam Complaint

CanIt-PRO harvests e-mail addresses from the WHOIS query and fills them in. It also composes an abuse complaint which includes all the information required to process the complaint, and includes the first 8kB of the spam message.

To send an abuse message follow these steps:

1. Edit the **To:** fields appropriately. CanIt-PRO may harvest inappropriate e-mail addresses; please verify that they are the correct addresses for abuse complaints. You can add multiple addresses in a single `To:` field by separating them with commas.
2. Enable the **Send** checkbox beside each **To:** address you want to complain to.
3. Edit the complaint text, if you wish.
4. Click **Send Complaint** to e-mail the spam complaint.

Chapter 5

Blacklists, Whitelists and Rules

CanIt-PRO allows you to make your own lists of senders, domains and hosts that are always allowed to send you mail, or never allowed to send you mail. It also lets you create custom rules and other types of rules. The following sections describe how to create these lists and rules.

5.1 The Sender Action Table

CanIt-PRO can take specific actions based on the sender's e-mail address. To see the sender list, click on **Rules** and then **Senders**. The sender page appears:

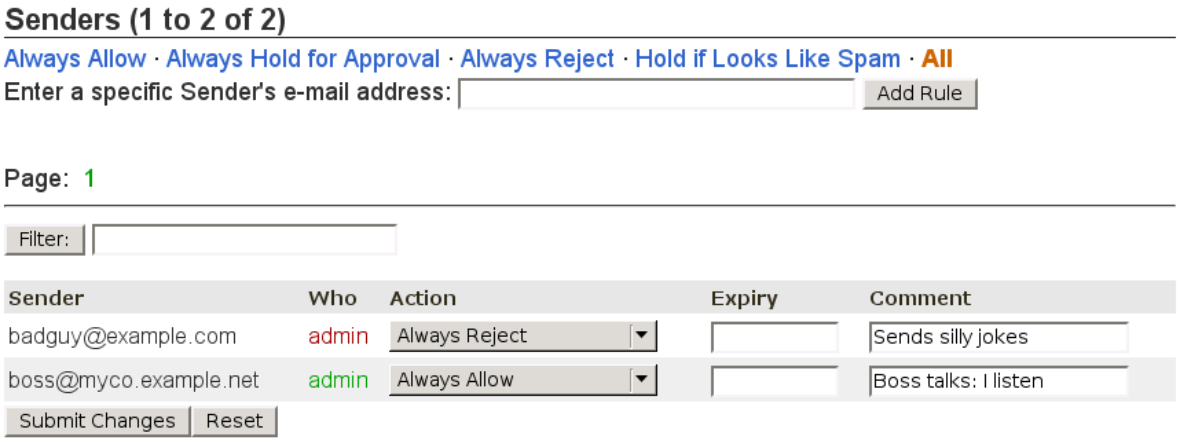


Figure 5.1: Sender Action Table

The columns in the table are:

Sender The e-mail address of a sender

Who The user who last modified the sender's disposition.

Action Shows the current action (which you can change). The possible actions are:

- **No Change** – keep the current action.
- **Always allow** – always allow mail from this sender without scanning for spam. (Dangerous attachments are still scanned and stripped.)
- **Always hold for approval** – mail from this sender is always held for approval, even if spam-scanning does not flag it as spam. (However, if spam-scanning *does* flag it as spam, then the message may be rejected if the spam score is high enough.)
- **Hold if looks like spam** – this is the default; mail from this sender will be held if it scores high enough on the spam scale.
- **Always reject** – messages from this sender are always rejected with a permanent failure code. The rejection happens early on in the SMTP dialog, before any message body is transmitted.
- **Delete from Table** – the sender is deleted from the table. Also, CanIt-PRO treats the sender as if the setting **Hold if looks like spam** had been used.

Expiry Allows you to set an expiry date after which the rule is automatically deleted. If you leave the expiry date blank, the rule will never be automatically deleted. Enter the date in the format YYYY-MM-DD. (If you have a modern browser, then clicking on the expiry field will pop up a handy JavaScript date selector to ease entry.)

Comment Allows you to enter a comment if you like. This can help you remember why you whitelisted or blacklisted a sender.

To set new actions, adjust the **New Action** entries appropriately and click **Submit Changes**.

If you want to set an action for an e-mail address that is not in the sender list, enter the address in the text box and press enter. You will then be given an opportunity to set the action for that address.

For convenience, if you click on a sender address in the message summary (Section 4.1) or incident display (Section 4.5), CanIt-PRO will take you to the sender entry for that address.

Click on **Always Allow**, **Always Hold for Approval**, **Hold if Looks Like Spam**, **Always Reject** or **All** to restrict the sender page to senders who are always allowed, always held, held if the message looks like spam, always rejected, or all senders, respectively.

Note: CanIt-PRO uses both the *Envelope Sender* and the **From:** header to determine the sender of an e-mail. In most e-mail clients, the envelope sender will appear in the **Return-Path:** header.

Note: You cannot use wildcards in the Sender Action Table. For example, rejecting `*@domain.com` will not work. Instead, reject `domain.com` in the Domain Action Table.

Note: CanIt-PRO will *ignore* a sender whitelist entry if the sender address matches the recipient address. This is to prevent problems if you whitelist your own address; spammers often fake spam so it appears to come from its victims.

5.1.1 Holding Unlisted Senders

CanIt-PRO can allow you to decide to only accept mail from a specific list of sender addresses, and to hold mail from all others. This essentially gives you the benefits of a challenge-response or sender opt-in system without requiring that senders perform any extra additional actions before sending you a message.

To use this feature:

1. Go to **Rules : Senders** and add the addresses of people you wish to receive mail from as **Always allow**.
2. Enable the **Hold mail from any sender not listed in Senders Table** setting under **Preferences : Stream Settings**.

Messages from the addresses you whitelisted will be allowed, and all messages from senders not specifically listed in the Sender Action Table will be held in your **Pending** trap, even if they score below your spam threshold.

5.2 The Domain Action Table

Just as it can make decisions based on the sender's address, CanIt-PRO can make decisions based just on the domain part of the address. (The domain part is everything after the `@` sign. For example, the domain part of `info@roaringpenguin.com` is `roaringpenguin.com`.)

To see the domain list, click on **Rules** and then **Domains**. The domain list appears:

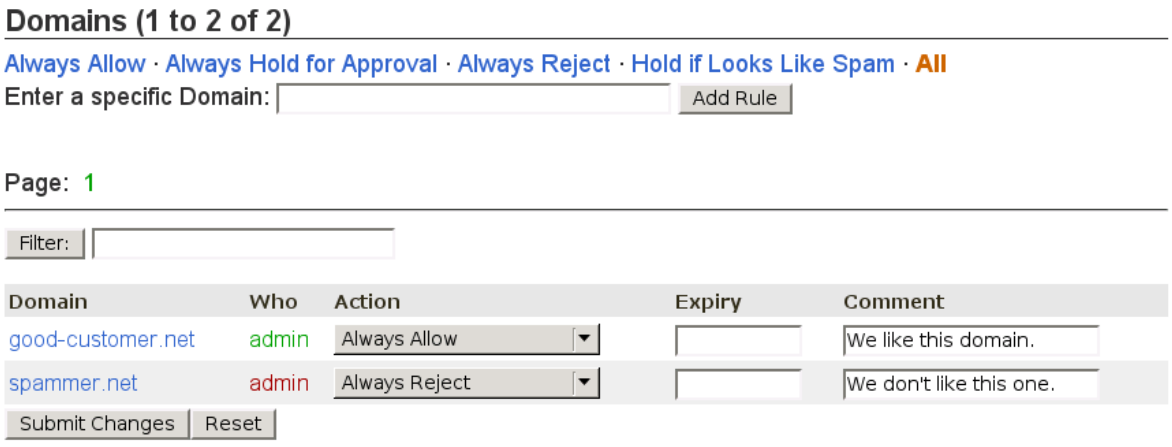


Figure 5.2: Domain Action Table

The columns and actions in the table have similar meanings to those the Sender Action Table (Section 5.1).

Click on **Always Allow**, **Always Hold for Approval**, **Hold if Looks Like Spam**, **Always Reject** or **All** to restrict the domain page to domains who are always allowed, always held, held if the message looks like spam, always rejected, or all domains, respectively.

Note: CanIt-PRO will *ignore* a domain whitelist rule if the domain of the sender is the same as (or a subdomain of) the domain of the recipient. This is to prevent problems if you whitelist your own domain; spammers often fake spam so it appears to come from the domain of its victims.

5.2.1 Domain Matching Rules

CanIt-PRO uses the same approach to match domains as Sendmail's access table does. Suppose you receive e-mail from `user@mail.sub.domain.net`. CanIt-PRO performs the following domain lookups:

1. `mail.sub.domain.net`
2. `sub.domain.net`
3. `domain.net`
4. `net`

and the first entry in the database is selected. Thus, if you disallow e-mail from `baddomain.com`, you also automatically block `bouncer.baddomain.com` and `spambox.baddomain.com`. However, you can explicitly allow `goodbox.baddomain.com` by adding another entry, because a domain with more components is more specific than (and takes preference over) one with fewer components.

5.3 The Network Action Table

CanIt-PRO can apply actions automatically based on the IP address of the SMTP relay host. To see the network list, click on **Rules** and then **Networks**:

Figure 5.3: Network Action Table

The columns and actions in the network table have similar meanings to those in the sender and domain tables, except that they are keyed on the IP address of the sending host. In addition, the network blacklist has an additional option, **Skip RBL Checks**. This option is almost the same as **Hold if looks like spam**, except that DNS-based blacklist lookups are disabled. This is useful, for example, if you receive legitimate mail from a host that ended up in a blacklist. You might not want to whitelist the host entirely, but you need a way to turn off the real-time blacklist lookup.

If you choose to hold mail from a network (whether you hold it always or only if it looks like spam), then domain and sender checks are performed, and may override the host check. (For example, if you tell CanIt-PRO to always hold mail from 172.20.201.32, but always accept mail from `friend@mycompany.com`, then mail from `friend@mycompany.com` relayed through 172.20.201.32 is accepted.)

A *network* is specified in CIDR notation as `a.b.c.d/bits`. The `bits` component can range from 8 to 32, and specifies how many left-most bits are significant. All of the right-most bits that are not significant *must* be zero. Here are some examples of CIDR networks:

- `192.168.2.1/32` specifies the single IP address `192.168.2.1`.
- `10.2.128.0/20` specifies the range from `10.2.128.0` through `10.2.143.255`
- `10.2.3.4/24` is *illegal* because the last 8 bits are not all zero.

For more information on CIDR notation, see http://tools.ietf.org/html/rfc4632#section-3.1.

5.4 Country Rules

CanIt-PRO can add scores to messages based on the country in which the sending relay is located.

Note: The CanIt-PRO administrator must have configured CanIt-PRO to download country-code data from Roaring Penguin for this feature to work. Consult the Administration Guide (section "Ruleset and Geolocation Data Updates") for details.

To create country scoring rules, click on **Rules** and then **Countries**. The country-code rule page appears:

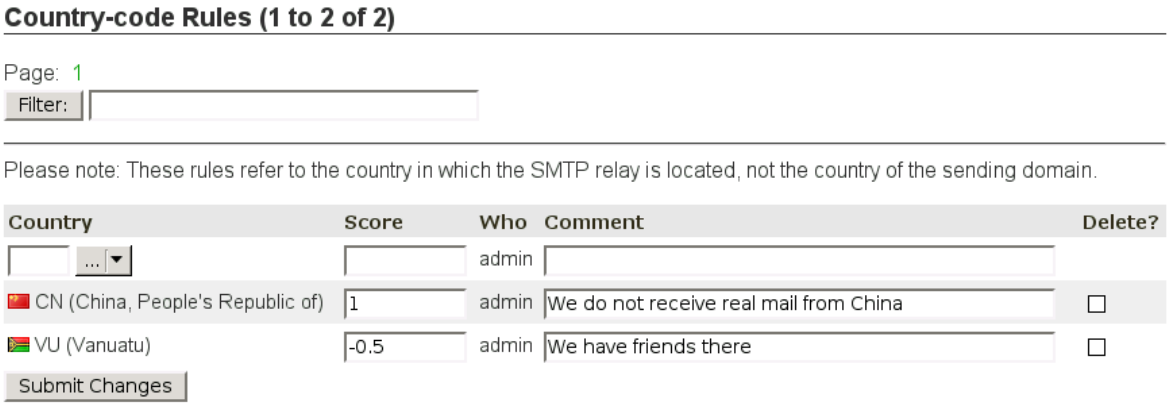


Figure 5.4: Country-Code Rules

To create a country-code rule:

1. Enter the two-letter ISO-3166 country code in the **Country** box. (These country-codes are listed at http://www.iso.org/iso/country_codes.) If you do not know the two-letter code for a country, select the country name from the pull-down list and the correct two-letter code will automatically be entered.
2. Enter the numerical score to add for messages originating from the country you chose. You can subtract points for a country by entering a negative score.
3. Optionally, enter a comment explaining why you created the rule.
4. Click on **Submit Changes** to add the rule.

Note that the **Filter:** box on the country-code rule page filters only by two-letter country code, not by country name.

5.5 Bulk Blacklisting and Whitelisting

Entering a large number of networks, domains or senders into the blacklist/whitelist tables can be time-consuming. CanIt-PRO provides an alternative interface for bulk entry.

To see the bulk entry page, click on **Rules** and then **Bulk Entry**:

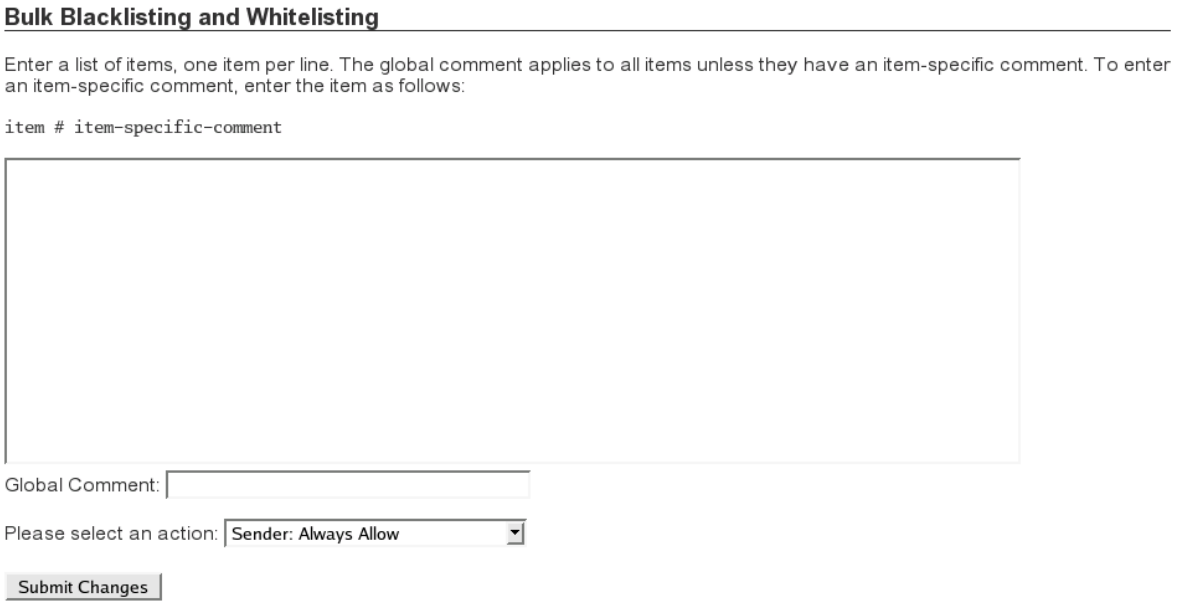

Bulk Blacklisting and Whitelisting
Enter a list of items, one item per line. The global comment applies to all items unless they have an item-specific comment. To enter an item-specific comment, enter the item as follows:
item # item-specific-comment
Global Comment:
Please select an action:
Sender: Always Allow
Submit Changes

Figure 5.5: Bulk Entry

- Enter the items you want to blacklist or whitelist, one per line. If you wish to enter item-specific comments, enter them following a pound symbol, like this:

  ```
  item # item-specific comment
  ```

  In the bulk-entry text box, blank lines and lines starting with a pound sign are ignored.

- If you want a global comment to apply to all items that lack an item-specific comment, enter the comment in the **Global comment** entry box.

- Select the action. Depending on your access rights, you can bulk-enter senders, networks and domains. Choose the appropriate entry type and action from the menu.

- Click **Submit Changes** to submit the bulk data.

5.6 MIME Types

CanIt-PRO allows you to hold or reject e-mail with attachments of certain MIME types. Some MIME types pose a risk, and you might want to hold or reject e-mail messages containing them. In particular, the `message/partial` MIME type may pose a risk, and we recommend you reject or hold it.

To see the MIME type list, click on **Rules** and then **MIME Types**:

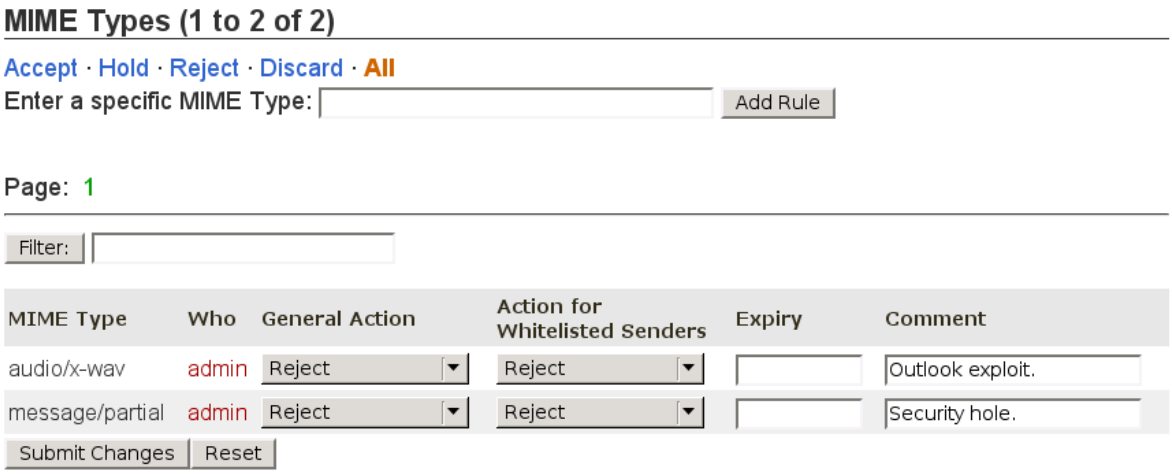


Figure 5.6: MIME Types

For each MIME type, you can **Accept**, **Hold**, **Reject** or **Discard** e-mail containing the type. Note that the default is **Accept**. This does not mean that mail will be specifically accepted regardless of other factors; it just means that it will not be rejected because of a MIME type.

The **Hold** setting causes e-mail containing parts of the specified type to be held in the trap, and **Reject** causes the e-mail to be rejected.

To add a new MIME type to the list, enter it in the "Enter a specific MIME type:" input box and press Enter. You can then adjust its setting and click **Submit Changes**.

Note that with MIME types, you can specify a different action for whitelisted senders. If a sender address, network, or domain is whitelisted, then the action in the **Action for Whitelisted Senders** column applies. Otherwise, the **General Action** applies. You might use this, for example, to hold images from most people, but permit them from anyone you have whitelisted.

MIME type rules may be set to expire by entering a date in the format YYYY-MM-DD in the **Expiry** box.

5.7 Filename Extensions

CanIt-PRO allows you to hold or reject e-mail with attachments whose filenames end in certain extensions. Some filename extensions may pose a risk to Windows machines.

To see the filename extension list, click on **Rules** and then **Filename Extensions**:

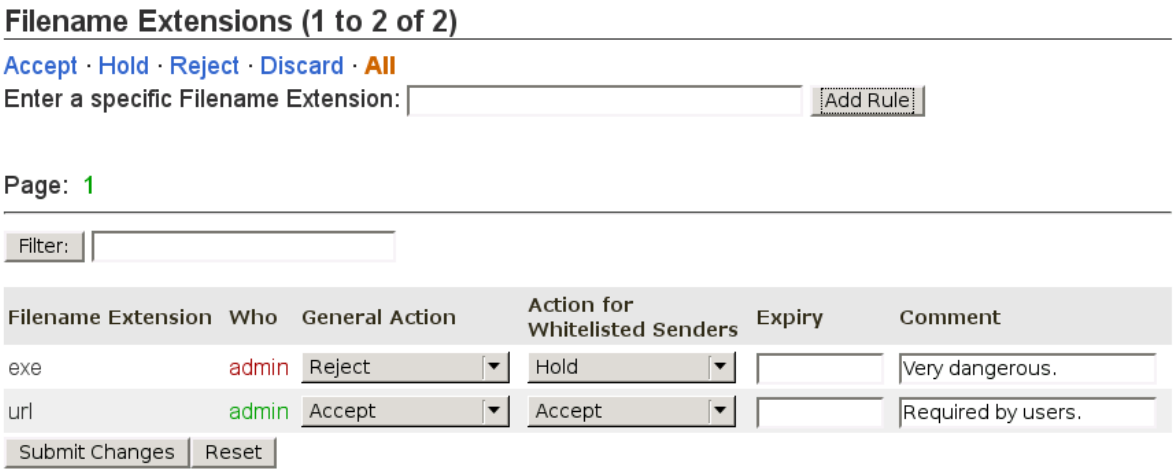


Figure 5.7: Filename Extensions

For each extension, you can **Accept**, **Hold**, **Discard** or **Reject** e-mail containing the extension. Note that the default is **Accept**. This does not mean that mail will be specifically accepted regardless of other factors; it just means that it will not be rejected because of an extension.

Note: Do *not* include the period in the extension. For example, if you want to block files ending in `.exe`, enter "exe", not ".exe". Filename extension matching is case-insensitive.

To enter a new extension in the list, enter it in the "Enter a specific filename extension:" input box and press Enter.

Filename extension rules may be set to expire by entering a date in the format YYYY-MM-DD in the **Expiry** box.

With filename extensions, as with MIME types, you can specify a different action for whitelisted senders. If a sender address, network, or domain is whitelisted, then the action in the **Action for Whitelisted Senders** column applies. Otherwise, the **General Action** applies. You might use this, for example, to hold ZIP files for most people, but allow them for anyone you have whitelisted.

5.7.1 Matching Entire File Names

In the Filename Extension list, you can match an entire file name by prefixing the name with "^". For example, the entry `^message.zip` will match if the entire filename is `message.zip` (using a case-insensitive comparison, of course.)

5.7.2 Matching All Attachments

In the Filename Extension list, you can match *all* attachments by using the extension `*` (a single asterisk). You can make specific entries to override the `*` actions.

5.8 Custom Rules

In addition to the built-in spam-detection rules, you can create your own custom rules which affect the spam score. To create your own rules, click on **Rules** and then **Custom Rules**:

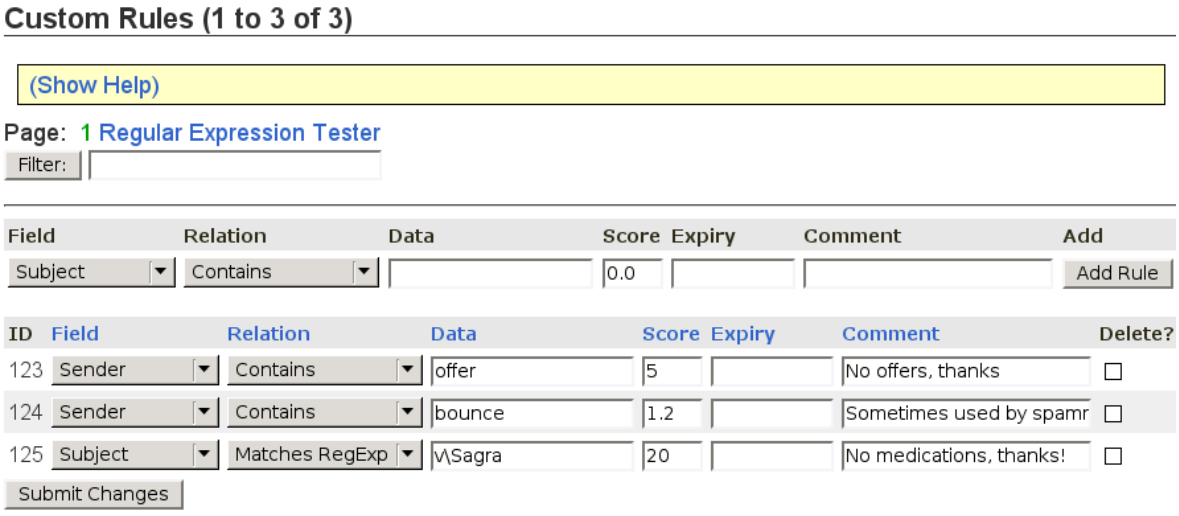

Custom Rules (1 to 3 of 3)
(Show Help)
Page: 1 Regular Expression Tester
Filter:
Field Relation Data Score Expiry Comment Add
Subject Contains 0.0 Add Rule
ID Field Relation Data Score Expiry Comment Delete?
123 Sender Contains offer 5 No offers, thanks
124 Sender Contains bounce 1.2 Sometimes used by spamr
125 Subject Matches RegExp \/\Sagra 20 No medications, thanks!
Submit Changes

Figure 5.8: Custom Rules

CanIt-PRO's custom rules allow you to adjust the spam score based on certain fields in each e-mail message. For each e-mail message, all of your custom rules are checked, and any which match have their score added to the spam score. Note that you can lower the spam score by specifying a negative number for a custom rule's score.

Note: CanIt-PRO custom rules are less efficient than built-in SpamAssassin rules. You should not create more than one or two hundred custom rules in a given stream or in the "default" stream or CanIt-PRO will be very slow. If you require that many rules, you should investigate coding them up as SpamAssassin rulesets.

If you enter a string in the "Filter:" box, CanIt-PRO will restrict the listing to those items that contain the string in the **Field**, **Relation**, **Data** or **Comment** column.

5.8.1 Fields

Each custom rule can examine a certain part of the mail message, called a *field*. The available fields are:

Subject The subject of the message.

Sender The SMTP envelope sender (what appears in the MAIL FROM: command; not necessarily what appears in the From: header.)

Recipient The SMTP envelope recipient (what appears in the RCPT TO: command; not necessarily what appears in the To: or Cc: headers.)

If you create a rule based on **Recipient**, the rule fires if any recipient matches.

HELO The argument the server gave to the SMTP "HELO" or "EHLO" command. Many spammers misguidedly think that if they provide your own server name in the HELO command, your machine is more likely to accept the mail. You can detect those spammers with a HELO rule.

Relay The canonical name of the sending relay, as determined by a reverse DNS lookup. If the lookup fails, the relay name is set to its IP address in square brackets, like this: `[127.0.0.1]`

RelayAddress The IP address of the sending relay.

Header Applies to all the header lines of the message. If any header matches the rule, then the rule matches. Please see Section 5.8.6 for more details.

Body Applies to the message body. Note that "Body" matches apply to decoded message parts, after any MIME encoding has been decoded. See Section 5.8.7 for more details.

RawBody Applies to the raw, undecoded message including all headers and the undecoded MIME body. In most cases, you should not use **RawBody** matching; instead, use **Body** matching.

5.8.2 Relations

Fields can be compared in several ways:

Contains activates a rule if the field contains the string you specify. The string-matching test is not case-sensitive, and word boundaries are ignored. Thus, the string "Roaring Penguin" is considered to contain "oAr".

Starts with activates a rule if the field starts with the specified string. Matching is not case-sensitive.

Ends with activates a rule if the field ends with the specified string. Matching is not case-sensitive.

Regexp matches considers the string you specify to be a Perl regular expression. If the field matches the regular expression (in a case-insensitive match), then the rule is fired. Please note that it is possible to write invalid regular expressions; these never match anything, but produce error messages in your mail log. You can also write regular expressions which take a long time to evaluate, so be careful.

Does not contain activates a rule if the field does *not* contain the specified string.

Is activates a rule if the field exactly equals the specified string, in a case-insensitive way.

Note that the last two comparisons (**Does not contain** and **Is**) are not likely to be useful for the Header, Body or RawBody fields.

5.8.3 Score

The score associated with a rule is added to the spam score if the rule matches. Negative scores may be useful; for example, if you want sensitive e-mail not to be trapped, you can inform people you trust to put a magic string (like `Confidential-394753486`) in the subject of the message. You could then create a rule:
If **Subject** contains `Confidential-394753486` then score **-200**.
which artificially lowers the message score, ensuring it will not be trapped.

5.8.4 Expiry

Custom rules may be set to expire by filling in a date (in the format YYYY-MM-DD) in the **Expiry** box. If you leave the **Expiry** box blank, the custom rule will never expire automatically.

5.8.5 Creating and Deleting Custom Rules

To create a custom rule:

1. Set the field to one of **Subject**, **Sender**, **Recipient**, etc.
2. Set the relation appropriately (**Contains**, **Starts with**, etc.)
3. Enter the string you want to match in the text box. For the **Regexp matches** relation, be sure to enter a valid Perl regular expression.
4. Enter the score adjustment value in the score box.
5. If you wish, enter explanatory notes in the **Comment** column.
6. Click **Submit Changes** to add the rule.

To delete a rule, simply enable the appropriate **Delete?** checkbox and click **Submit Changes**.

If you supply a rule with a very large positive score, you can configure CanIt-PRO to automatically reject e-mail. The default setting rejects mail scoring over 2000 (which never actually happens without custom rules.) You can create a custom rule with a score of 2000 or more to auto-reject mail.

Similarly, a custom rule with a negative score of around -2000 will always allow mail it matches to come through without being trapped.

5.8.6 Header Matching

A custom rule matching on the **Header** tests each header line, and if one matches, the rule is considered to match. It is most useful to use **Regexp match** with headers, because you need to match both the header name and value.

For example, suppose you want to match `bad@spammer.net` in the `From:` header. (This is *not* the same as a **Sender** rule, because the **Sender** rule uses the envelope sender too.) You could create a rule like this:
If **Header** Regexp matches `^From:.*bad@spammer.net` then score **10**

5.8.7 Body Matching

A custom rule matching **Body** or **RawBody** tests each body line, and if one matches, the rule matches. Note, therefore, that you cannot match phrases that span multiple lines.

A **Body** rule reads the decoded MIME body parts, while a **RawBody** rule uses the complete undecoded MIME message, including headers.

For example, if you want to add 20 to all messages containing "horny" in the body, create a rule like this:
If **Body** Contains `horny` then score **20**.

5.9 RBL Rules

The term *RBL* (as used in CanIt-PRO) stands for "real-time blacklist" or "real-time blocklist". An RBL is a DNS-based list of known-bad IP addresses. Whenever CanIt-PRO is processing an SMTP session, it can look up the originating host in a number of RBLs, and take action if the host is on the RBL.

The CanIt-PRO administrator must first set up a *Master List* of RBLs. This list is a list of all possible RBLs that are available to you. You then can make rules for the various RBLs.

To create RBL rules, click on **Rules** and then **RBL Rules**. The RBL Rules page appears:

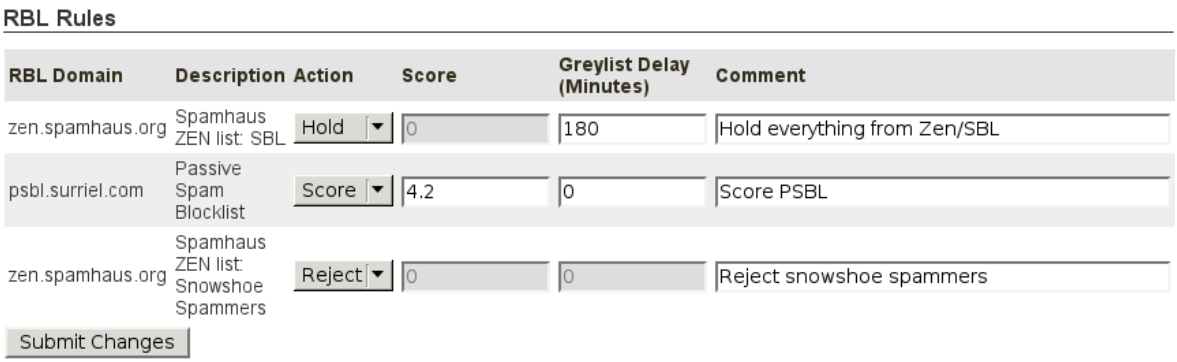


Figure 5.9: RBL Rules

The RBL Rules page lists all of the RBLs in the Master List, along with how CanIt-PRO will use them. To create an RBL rule for a specific RBL domain:

1. Select an action to take if the sending relay is blacklisted by the RBL. The possible actions are:
   - **Ignore** — the RBL is not used at all.
   - **Hold** — mail from a host in the RBL will be held in the trap.
   - **Reject** — mail from a host in the RBL will be rejected.
   - **Score** — points will be added to the score for any mail from a host in the RBL.

2. If you selected an action of **Score**, enter the number of points to add in the **Score** box.
3. If you selected an action of **Score** or **Hold**, you can optionally extend the amount of time a machine is greylisted if it is in the RBL. If you don't know what value to use, enter a value of zero. Otherwise, enter a value from 1 to 2880; this will force an RBL-listed machine to remain in greylisting for that many minutes before being allowed to pass greylisting.
4. If you like, enter a comment in the **Comment** box so you can describe why you made the rule the way you did.
5. Click **Submit Changes** to activate the rule.

5.10 Mismatch Rules

Mismatch rules are special rules that check for a mismatch between the sender's domain and the SMTP relay's domain. These rules are *not* recommended for general use, but are very useful at stopping a lot of spam in certain specific situations.

A mismatch rule allows you to hold or reject e-mail, or add to the spam score, if the sending relay's hostname (as determined by a DNS lookup) does not end in the same domain as the sender's supposed e-mail address.

In general, it is perfectly valid for this mismatch to occur, and you should not block mail just because the relay hostname doesn't match the sender's domain. However, many spammers use fake `hotmail.com`, `yahoo.com`, `aol.com` and `earthlink.net` addresses. All of those popular services have good reverse-DNS configurations, and their outgoing relay host names all end in the appropriate domain name. It can be very effective to hold or block mail from these (and other) services if the relay host name does not match the sender domain name.

To enter mismatch rules, click on **Rules** and then **Mismatch Rules**:

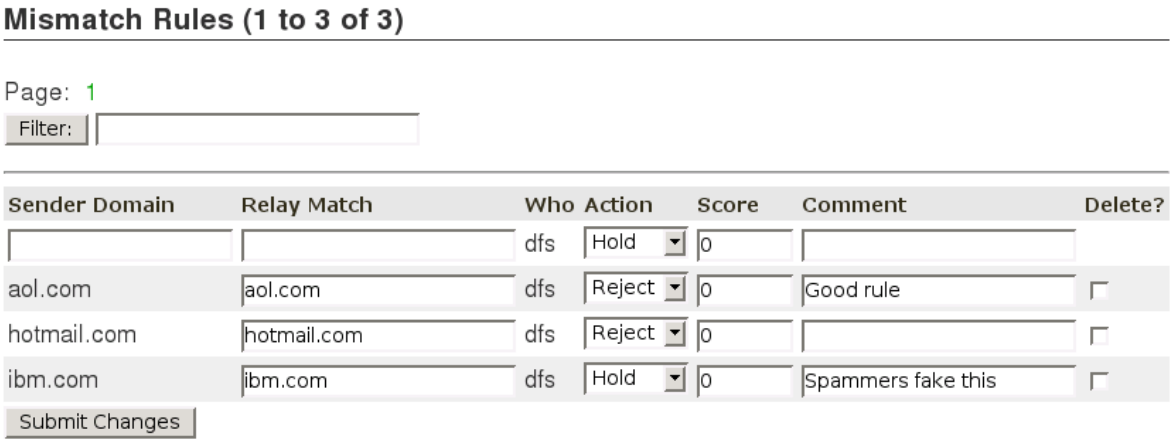


Figure 5.10: Mismatch Rules

If you enter a string in the "Filter:" box, CanIt-PRO will restrict the listing to those items that contain the string in the **Sender Domain** or **Relay Match** column.

To add a mismatch rule:

1. Enter the domain in the **Sender Domain** box.
2. Enter the string which the sending relay must end with in the **Relay Match** box. If you leave the **Relay Match** box empty, it defaults to the **Sender Domain**. You can enter a comma-separated list of domains in the **Relay Match** box; as long as the relay matches *one* of the domains, it will be accepted.

   For example, mail from `msn.com` might come from an `msn.com` or `hotmail.com` relay. In this case, you would put `msn.com, hotmail.com` in the **Relay Match** box.
3. Set the **Action** to "Hold" if you want to hold mismatched messages in the trap, or "Reject" if you want to reject them outright. If you'd rather just add to the spam score, set **Action** to "Score" and enter the amount you want added in the **Score** box.
4. If you wish, add explanatory notes in the **Comment** box.
5. Click on **Submit Changes** to add the rule.

To delete a rule, simply enable the appropriate **Delete?** checkbox and click **Submit Changes**.

In the example in Figure 5.10, CanIt-PRO will reject all e-mail from aol.com and hotmail.com unless it comes from a relay whose hostname ends with the corresponding domain. Mail from ibm.com that comes from a host whose name does not end with ibm.com will be held in the trap.

Just like with domain blacklists and whitelists, CanIt-PRO checks mismatch rules using the domain matching rules in Section 5.2.1 on page 36. That is, if mail is received from `user@mail.sub.domain.net`, then CanIt-PRO looks for the following mismatch rules:

1. `mail.sub.domain.net`
2. `sub.domain.net`
3. `domain.net`
4. `net`

To reiterate: Mismatch rules are not appropriate for general use. Even for the example domains, there may well be legitimate reasons for an aol.com user to relay mail through a non-aol.com server. It's up to you to balance the highly-effective nature of mismatch rules against the possibility of holding or rejecting valid mail.

5.11 SPF Rules

SPF (Sender Policy Framework) is a more sophisticated version of Mismatch Rules. SPF allows the owners of a domain to assert which hosts are allowed to originate e-mail claiming from that domain.

For example, the domain `aol.com` has an SPF record that lists which hosts ordinarily send out AOL mail. If you receive mail from a host not in AOL's list of approved senders, it is probably faked.

For more details on SPF, please see http://www.openspf.org/

To add SPF rules to CanIt-PRO, click on **Rules** and then **SPF Rules**:

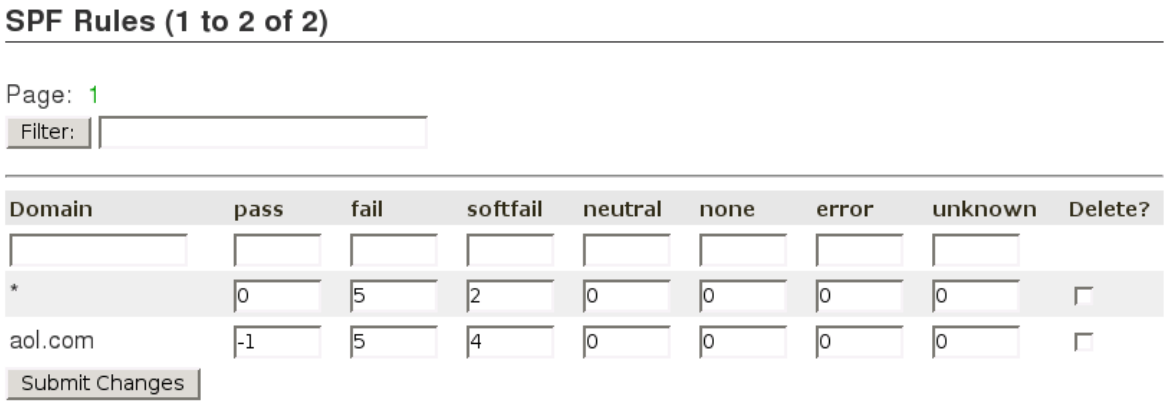


Figure 5.11: SPF Rules

If you enter a string in the "Filter:" box, CanIt-PRO will restrict the listing to those items that contain the string in the **Domain** column.

5.11.1 How SPF Queries Work

An SPF query is a DNS query looking for a specific record. The SPF query takes as input the sender address, the IP address of the sending host, and the argument to the SMTP HELO command. It can return one of seven values:

- **pass** means that the specified host is authorized to send mail for the domain.
- **fail** means that the specified host is not authorized to send mail for the domain, and that the domain administrators would prefer you to reject the mail.
- **softfail** means that the specified host is not authorized to send mail for the domain, but that the domain administrators want you to accept the mail anyway because it may be legitimate for some senders to relay through other machines.
- **neutral** means that the domain administrator has no opinion about the legitimacy of the sending host.
- **none** means that there is no SPF record for the domain.
- **error** means that the DNS lookup encountered a temporary error.
- **unknown** means that the SPF record has a syntax error.

CanIt-PRO allows you to add different scores for the various query results. We recommend adding 5 points for **fail** and 2 points for **softfail**, and leaving all other scores at zero. You may cautiously subtract points for **pass**, but we recommend doing this only for selected domains.

5.11.2 Entering SPF Rules

To enter an SPF rule:

1. Enter the domain the rule should apply to in the **Domain** entry box. If you enter `*` in the **Domain** entry box, then the rule applies to all domains unless there is a more-specific entry for the domain.

   As with domain rules, SPF rules are searched by stripping domain components until a match is found. For example, for the domain `x.example.com`, CanIt-PRO searches for SPF rules in the following order and stops when the first rule is found:

   (a) `x.example.com`
   (b) `example.com`
   (c) `com`
   (d) `*`

2. Enter the scores for each return code in the appropriate columns. If you leave a score entry box blank, zero is used.

3. Click on **Submit Changes** to add the rule.

To delete an SPF rule, simply enable the appropriate **Delete?** checkbox and click **Submit Changes**.

5.11.3 Vouch by Reference

RFC 5518 (http://tools.ietf.org/html/rfc5518) specifies a protocol called *Vouch By Reference* or VBR. The allows a trusted domain to list a set of domains whose SPF records should be trusted. Rather than entering dozens of domains in the SPF rule form, you can ask CanIt-PRO to use a trusted vouch-by-reference domain. To enter a VBR rule, use the following in the **Domain** field: **vbr:*domain.example.com***

When CanIt-PRO sees a **vbr:*domain.example.com*** rule, it applies the following process:

1. Given a domain **example.org**, it looks up a DNS TXT record for **example.org._vouch.domain.example.com**

2. If such a record is found and matches the specification in RFC 5518, then CanIt-PRO applies the scores associated with the VBR entry.

Note that an exact match overrides a VBR lookup. Also note that VBR lookups are relatively expensive and should be used sparingly.

5.12 DKIM Rules

DKIM stands for "DomainKeys Identified Mail." DKIM has a similar goal to SPF—it allows organizations to declare in a secure way that they are responsible for a particular email message—but uses a very different mechanism.

A sender using DKIM *signs* outgoing messages with a private key. The signature covers certain message headers and (usually) the message body. The sender also publishes the public key corresponding to the private key using a special DNS record.

A recipient *verifies* the DKIM signature and takes action based on the verification result. If a DKIM signature verifies correctly, the receiver can be very confident that the domain purporting to originate the email message is in fact responsible for it. If the DKIM signature fails, then the message either didn't originate with the domain or has been altered in transit.

For more information on DKIM, see http://www.dkim.org/

To add DKIM rules to CanIt-PRO, click on **Rules** and then **DKIM Rules**:

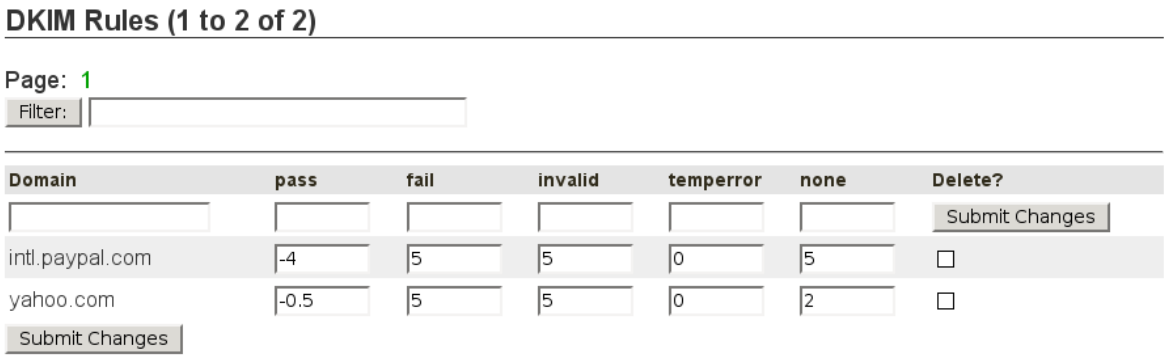


Figure 5.12: DKIM Rules

If you enter a string in the "Filter:" box, CanIt-PRO will restrict the listing to those items that contain the string in the **Domain** column.

CanIt-PRO lets you add or subtract points based on the results of DKIM signature verification. The possible results are:

pass The message had a DKIM signature and it was correctly verified.

fail The message had a DKIM signature, but the signature was incorrect.

invalid The message had a DKIM signature, but it was invalid (ie, malformed or corrupt). No verification could be attempted.

temperror There was a temporary failure in DKIM signature verification. (This could happen if the public key cannot be retrieved.)

none The message did not have a DKIM signature at all.

You can use different scores for different domains. In the examples in Figure 5.12, you can see that we trust `intl.paypal.com` quite a bit, so subtract 4 points for a DKIM-verified message. Since we always expect Paypal messages to have a valid DKIM signature, we add 5 points for bad, invalid or nonexistent DKIM signatures.

We trust `yahoo.com` quite a bit less, so we only subtract 0.5 points for a validly-signed message. We add 5 points for bad or invalid signatures, but only two points for missing signatures. Some people use their Yahoo email addresses without relaying through Yahoo's servers, so it is reasonably common for their messages to lack a signature.

To enter a DKIM rule:

1. Enter the domain the rule should apply to in the **Domain** entry box. If you enter `*` in the **Domain** entry box, then the rule applies to all domains unless there is a more-specific entry for the domain.

   As with SPF rules, DKIM rules are searched by stripping domain components until a match is found. For example, for the domain `x.example.com`, CanIt-PRO searches for DKIM rules in the following order and stops when the first rule is found:

   (a) `x.example.com`
   (b) `example.com`
   (c) `com`
   (d) `*`

Note: CanIt-PRO uses the domain specified in the DKIM signature since that is the domain taking responsibility for signing the message. This domain *may or may not* be the same as the domain of the sender's email address.

2. Enter the scores for each return code in the appropriate columns. If you leave a score entry box blank, zero is used.

3. Click on **Submit Changes** to add the rule.

To delete an DKIM rule, simply enable the appropriate **Delete?** checkbox and click **Submit Changes**.

5.12.1 Vouch by Reference

DKIM rules can use Vouch by Reference in a manner similar to SPF rules. See Section 5.11.3 for details.

5.13 Blacklisting Recipients

Often, a large volume of spam is destined for nonexistent users at your site. This is usually because users leave the company, but spammers still have their old e-mail addresses.

Ideally, the CanIt-PRO machine will check the validity of recipient addresses, by checking against your real SMTP server or by validating against LDAP, Active Directory, or some other backend system with full knowledge of your valid addresses. Unfortunately, in some cases it may not be possible to validate against another system.

As a workaround for this, CanIt-PRO lets the administrator blacklist recipients. If you notice a lot of spam trapped for a nonexistent recipient, simply blacklist that recipient. To blacklist a recipient:

- Click on **Rules** and then **Blacklisted Recipients**.
- Enter the full e-mail addresses of the recipient you wish to blacklist. You can enter more than one address; just put each address by itself on a line.
- Click **Blacklist Recipient(s)**

If mail comes in for a blacklisted recipient, CanIt-PRO fails the RCPT TO: command for that recipient.

To remove a recipient from the blacklist, click on the **Delete** link near the recipient's e-mail address in the blacklisted recipients table.

The list of blacklisted recipients is kept on a per-stream basis. When testing if an address is blacklisted, CanIt-PRO first determines which stream the address would map to, and it then looks up that stream's list of blacklisted recipients.

Although a stream administrator can blacklist any address, CanIt-PRO will ignore addresses that don't map to that stream. For example, if the stream administrator for `user1` blacklists the address `user2@domain.net` (which presumably maps to a different stream), CanIt-PRO will ignore the entry.

The CanIt-PRO administrator can globally blacklist recipients by placing the blacklisted addresses in the `default` stream.

Note: CanIt-PRO refuses to obey a blacklist on the special address `postmaster`, because this address is required to accept mail according to the SMTP standard.

5.14 Enumerating Valid Recipients

If you have a relatively small site, you can enter a list of valid recipients into CanIt-PRO, and CanIt-PRO will not accept mail for recipients unless they are in the table of valid recipients. *Be sure to enter all your valid addresses, including aliases and "role" addresses into the Valid Recipients Table.*

To enter a list of valid recipients:

- Click on **Rules** and then **Valid Recipients**
- Enter the full e-mail addresses (one per line) of valid recipients. Note that you can enter either a complete address (like `user@domain.com`) or just the local part (`user`). If you just enter the local part, then any e-mail address whose local part is found in the table will be accepted.
- Click **Add Recipient(s)**

Normally, CanIt-PRO does *not* consult the table of Valid Recipients.

If you want the table to be used for a particular stream, set the "Only accept mail for accounts in the Valid Recipients table" Stream Setting to **Yes**. You should only enable "Only accept mail for accounts in the Valid Recipients table" in the **default** stream if you wish to enable Valid Recipients checking for *all* streams. Enabling it globally is not recommended in most cases.

The list of valid recipients is kept on a per-stream basis. When looking up a recipient, CanIt-PRO first determines which stream the address would map to, and then looks the address up in that stream's list of valid recipients.

The CanIt-PRO administrator can globally enter valid recipients by placing the addresses in the `default` stream.

Note that if your CanIt-PRO machine processes outgoing mail, you should ensure that outgoing mail is streamed to a stream that does *not* check the Valid Recipients Table.

Note: CanIt-PRO always treats the special address `postmaster` as valid, because this address is required to accept mail according to the SMTP standard.

5.15 Importing and Exporting Rules

CanIt-PRO can export your rules in *comma-separated value* (CSV) format. This format can be manipulated by a variety of software such as spreadsheets and database programs. CanIt-PRO can also import rules in CSV format, allowing for efficient bulk creation of rules.

5.15.1 Exporting Rules

To export rules, click on **Preferences** and then **Export Rules**. The Export Rules screen appears:

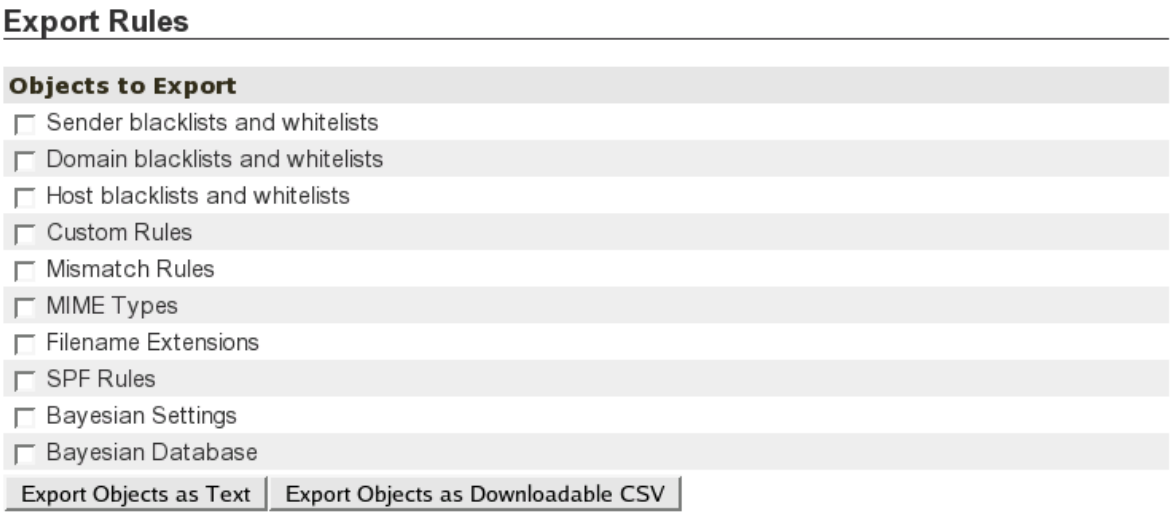


Figure 5.13: Export Rules

1. Select all of the rules you wish to export by enabling the appropriate checkboxes.
2. Click on **Export Objects as Text** to view the CSV file as a plain-text file in your browser. Click on **Export Objects as Downloadable CSV** if you want your browser to prompt you to save the text to a file.

The resulting CSV file can be imported into a spreadsheet program such as Open Office "calc" or other popular spreadsheet software.

5.15.2 Format of the Exported Rules

Each rule type in the CSV file has a specific layout. The fields are as follows:

- For sender blacklists and whitelists, the fields are:
  1. `Sender` – The literal text `Sender`.
  2. *stream* – The stream containing the rule.
  3. *address* – The sender's address.
  4. *action* – The action to associate with the address (one of `allow-always`, `hold-always`, `hold-if-spam` or `reject`.)
  5. *who* – The user ID of the person who created the rule.
  6. *comment* – Any comment attached to the rule.
- For domain blacklists and whitelists, the fields are:
  1. `Domain` – The literal text `Domain`.
  2. *stream* – The stream containing the rule.
  3. *domain* – The domain.
  4. *action* – The action to associate with the domain (one of `allow-always`, `hold-always`, `hold-if-spam` or `reject`.)
  5. *who* – The user ID of the person who created the rule.
  6. *comment* – Any comment attached to the rule.
- For network blacklists and whitelists, the fields are:
  1. `Network` – The literal text `Host`.
  2. *stream* – The stream containing the rule.
  3. *network* – The network address in CIDR notation.
  4. *action* – The action to associate with the network (one of `allow-always`, `hold-always`, `hold-if-spam`, `no-rbl` or `reject`.)
  5. *who* – The user ID of the person who created the rule.
  6. *comment* – Any comment attached to the rule.

- For custom rules, the fields are:
  1. `Custom` – The literal text `Custom`.
  2. *stream* – The stream containing the rule.
  3. *field* – The field associated with the rule.
  4. *relation* – The relation associated with the rule.
  5. *data* – The string data associated with the rule.
  6. *score* – The score to assign to the rule.
  7. *comment* – Any comment attached to the rule.
- For mismatch rules, the fields are:
  1. `Mismatch` – The literal text `Mismatch`.
  2. *stream* – The stream containing the rule.
  3. *domain* – The domain associated with the rule.
  4. *match* – A list of allowable domains for the relay host.
  5. *action* – The action to take if the rule is fired.
  6. *who* – The user-ID of the person who created the rule.
  7. *score* – The score associated with the rule.
  8. *comment* – Any comment attached to the rule.
- For MIME type rules, the fields are:
  1. `MIME` – The literal text `MIME`.
  2. *stream* – The stream containing the rule.
  3. *mimetype* – The MIME type.
  4. *action* – The action to associate with the MIME type.
  5. *who* – The user ID of the person who created the rule.
  6. *comment* – Any comment attached to the rule.
- For filename extension rules, the fields are:
  1. `Extension` – The literal text `Extension`.
  2. *stream* – The stream containing the rule.
  3. *extension* – The filename extension.
  4. *action* – The action to associate with the extension.
  5. *who* – The user ID of the person who created the rule.
  6. *comment* – Any comment attached to the rule.
- For Bayesian settings, the fields are:
  1. `Bayes` – The literal text `Bayes`.
  2. *stream* – The stream containing the rule.
  3. *percentage* – The percentage probability associated with the rule.
  4. *score* – The score associated with the rule.

5.15.3 Importing Rules

CanIt-PRO can import CSV files that are in the format described in Section 5.15.2 earlier. To import rules, click on **Preferences** and then **Import Rules**. The Import Rules page appears:

Figure 5.14: Import Rules

1. Enter the name of a file to upload in the text box. Use the **Browse...** button to browse your local file system to find a file.
2. Choose what to do in case of a conflict. The default, **Preserve Original**, means that if the CSV file contains a rule that conflicts with an existing rule, the existing rule is retained. Alternatively, you can choose **Overwrite**, which overwrites any conflicting rules with rules from the CSV file.
3. Click on **Import Objects** to import the rules.

Note: CanIt-PRO expects the CSV file to follow *precisely* the format described in Section 5.15.2. Any lines in the file that deviate from the format are silently ignored.

During rule importing, CanIt-PRO *ignores* the "stream" field in the CSV file. All rules are imported into the current stream.

5.16 Reviewing the Change History

Many rule pages feature a **Show Changes** link near the top of the page. Click on the link to see the *Change History* for the page:

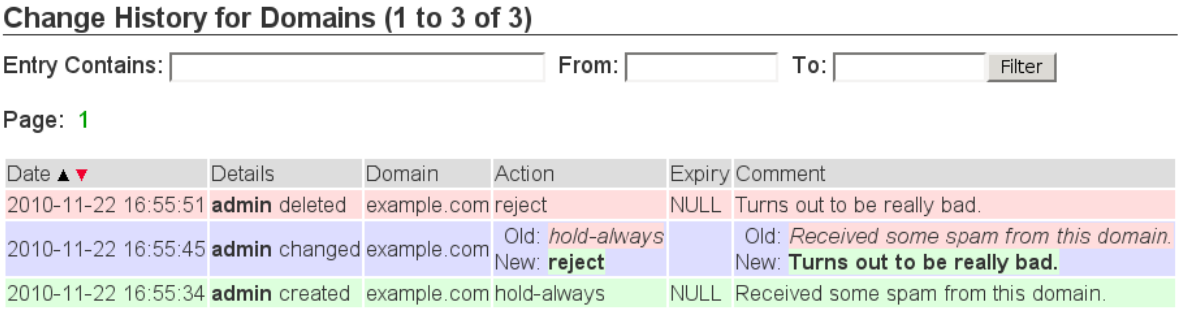

Change History for Domains (1 to 3 of 3)
Entry Contains:
From:
To:
Filter
Page: 1
Date ▲▼
Details
Domain
Action
Expiry
Comment
2010-11-22 16:55:51 admin deleted example.com reject NULL Turns out to be really bad.
2010-11-22 16:55:45 admin changed example.com Old: hold-always New: reject Old: Received some spam from this domain. New: Turns out to be really bad.
2010-11-22 16:55:34 admin created example.com hold-always NULL Received some spam from this domain.

Figure 5.15: Change History

Figure 5.15 shows a sample change history for the **Rules : Domains** page. By default, the change history is sorted from newest change to oldest change, so it should be read from bottom to top. Here's how to read the example in Figure 5.15:

- At 16:55:34, the user "admin" created a domin rule for **`example.com`**. The rule was to always hold mail for that domain.
- At 16:55:45, "admin" edited the rule. She changed the always-hold setting to always-reject and updated the comment.
- At 16:55:51, "admin" deleted the rule.

Within a Change History page:

- To restrict the data displayed, enter some search text in the **Entry Contains** field and press **Filter**. Only entries that contain the search string in any column to the right of **Details** will be displayed.
- To restrict the date range, enter dates in the form YYYY-MM-DD in either or both of the **From** and **To** fields. CanIt-PRO will only display changes that fall within the specified date range. You can combine date restrictions with search text to further restrict the display.

Chapter 6

Preferences

6.1 Preferences

CanIt-PRO allows each user to customize certain aspects of the Web-Based GUI. To change your preferences, click on the **Preferences** link:

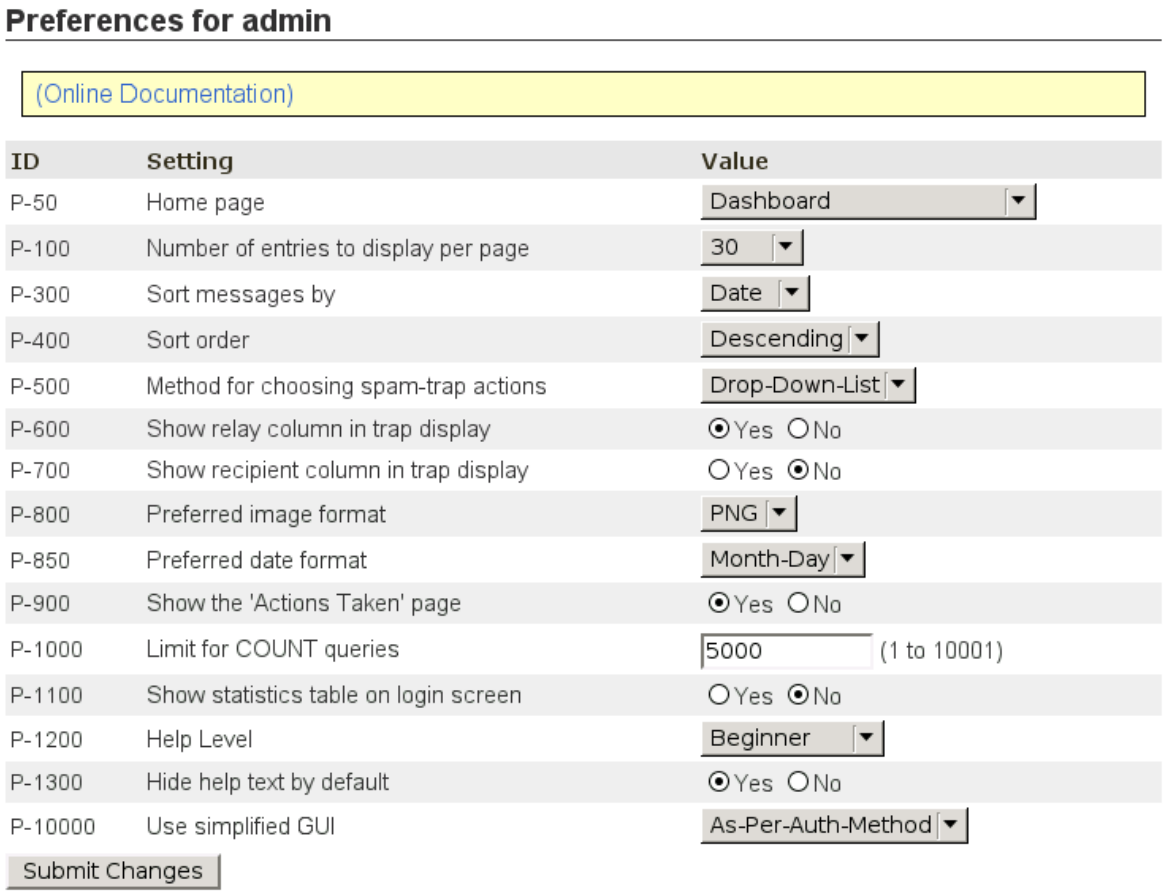


Figure 6.1: Preferences

The preferences you can change are:

Home page controls the page you see when you visit the base CanIt-PRO URL.

Expire "Remember Me" information after controls how long CanIt-PRO remembers you if you enable the "Remember Me" checkbox on the login page. Note that you should *never* use the "Remember Me" feature on a public computer; use it only on a workstation to which you alone have access.

Number of entries to display per page controls the number of messages per page in the message summary. Allowable values are 10, 30, 50, 100 or 200.

Sort messages by lets you sort messages either by date or by spam-scanning score.

Sort order controls the sort order (ascending or descending).

Method for choosing spam-trap actions controls the type of graphical object you use to accept or reject messages. The "Drop-Down-List" style offers a drop-down list of choices, while the "Checkbox" style offers two or three buttons to accept or reject messages (or leave them as-is.)

Show relay column in trap display If you select **No**, then the "Relay" column is not shown in the spam trap display. This may improve the layout on small screens.

Show recipient column in trap display If you select **Yes**, then an extra "Recipient" column is shown in the spam trap display. Only the first recipient is shown; if there are more than one, then an elipsis (. . .) is displayed. Note that you cannot sort the trap display by recipient.

Preferred image format CanIt-PRO normally uses PNG images for its GUI. If your browser has trouble displaying PNG images, you can use JPEG images instead.

Show the "Actions Taken" page If you select **Yes**, then when you take actions against messages, senders, and so on, CanIt-PRO displays a summary page describing the actions taken. If you select **No**, then CanIt-PRO skips this summary page, taking the specified actions and returning to the original page immediately.

Limit for COUNT queries On large spam traps, it may take a long time for the database queries that count items, such as the number of messages, number of sender rules, etc. If you set this preference to a number from 500 to 10,000, then CanIt-PRO does not fully count items higher than the specified number. For example, if your trap contains 1877 messages, but you set this limit to 1000, then CanIt-PRO simply displays "More than 1000" for the number of messages.

If you set this limit to the "magic" value 10,001, then CanIt-PRO does not limit how high it will count.

If you set the limit to the other "magic" value of 1, then CanIt-PRO eliminates most COUNT queries. While this makes the interface somewhat less friendly, it can speed things up tremendously on busy installations.

Show statistics table on login screen If you set this to **Yes**, then CanIt-PRO displays a summary of the contents of the trap. By default, this is turned off, because the query to generate the summary can take a considerable amount of time on a large trap.

Help Level Some CanIt-PRO pages have built-in help text. You can set the level of help to one of:

- **Beginner** – the most verbose form of help text.
- **Intermediate** – somewhat less verbose help text.
- **Expert** – very terse help text.
- **None** – no help text at all

Hide help text by default By default, the help text for each page is hidden, and there is a "Show Help" link that reveals the help text. This is to minimize the screen area taken up by help text, and to keep it as unobtrusive as possible. However, if you prefer to see the help by default, set this setting to **No**.

Use simplified GUI If you select **Yes**, then you are given only a very simple interface to CanIt-PRO. See Chapter 2 for details.

To change your preferences, fill in the correct values for each preference and then click **Update Preferences**.

6.2 Changing Default Preferences

If you are the CanIt-PRO administrator, you can enter a user name in the **Changing preferences for user:** box. This allows you to change preferences for other users. If you enter "*" (a single asterisk) as the user name, then any preferences you set become the default preferences for everyone. (Individual users can still override them.) If you enter "*root*" as the user name, then any preferences you set become the default preferences for users with root privilege.

6.3 Changing your Password

To change your password, click on **Preferences** and then **Change Password**.

Note: Only users in CanIt-PRO's user database can change their passwords. If a user was authenticated via an external authentication method, the **Change Password** link is not present.

To change the password:

1. Enter the new password in the **Enter new password:** box.
2. Enter the new password again in the **Re-enter new password:** box.
3. Enter your old password in the **Enter your existing password:** box.
4. Click **Change Password**

6.4 Quick Links

Because of the hierarchical arrangement of CanIt-PRO Web pages, it may take two clicks to get to a page. Some pages allow you to add them to a personal menu of "Quick Links".

For example, go to the **Rules : Custom Rules** page. At the bottom of the page is a button called **Add to Quick Links**.

Click on that button, and the Custom Rules page will be added to your own personal menu of quick links. In this way, you can make pages you access frequently available from any other page with a single click.

To remove a page from the Quick Links menu, visit that page and click on **Remove from Quick Links** at the bottom of the page. To clear out all your quick links, click on **Clear Quick Links**. Confirm the clearing by clicking on **Really Clear Quick Links**.

Note that not all pages are quick-linkable; any page that is immediately reachable from the top-level menu is not quick-linkable, and neither is a page that depends on user input or form data.

Quick Links are maintained on a per-user basis, so different users can have their own sets of quick links, according to how they use CanIt-PRO most effectively.

Chapter 7

Reports

CanIt-PRO provides various reports which help you determine the major sources of spam. To view the reports, click on the **Reports** link. The Statistics Page appears.

Note: If the system administrator has disabled real-time reports, then the statistics page will not appear. Instead, you will be able to select from various types of reports based on spam trap data.

7.1 Statistics

CanIt-PRO keeps statistics about the disposition of e-mail messages. To view the statistics, click on **Reports** and then **Statistics**. The Statistics Page appears:

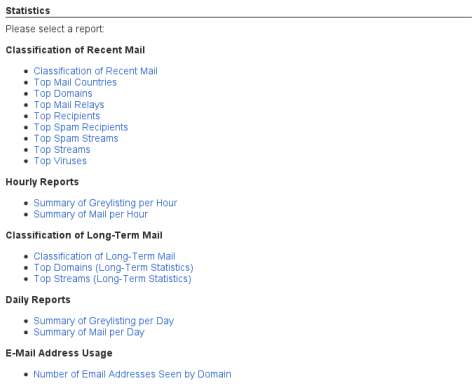


Figure 7.1: Statistics

There are five basic types of statistical reports:

1. *Classification of Recent Mail* reports. These reports classify recently-received e-mail and present the classifications as HTML tables and pie charts.
2. *Hourly* reports. These reports show a breakdown of recently-received e-mail by hour.

3. *Classification of Long-Term Mail* reports. These reports are similar to the Classification of Recent Mail reports, but operate over longer time spans. There are also fewer reports available because some of the data in the "recent mail" tables is summarized in the "long-term mail" tables, causing some details to be lost.

4. *Daily* reports. These reports break down e-mail by day. Daily reports cover a longer period of time than hourly reports.

5. *Usage* reports. These reports track the number of valid e-mail addresses seen in the last 60 days, broken down by domain.

Most of the reports can take parameters which allow you to select which mail to report on. Some parameters are particular to a given report, but one that is common to most reports is the **Domain** parameter. To restrict queries by domain:

- Enter a comma-separated list to only see mail to the given domains. For example, entering `example.com, example.net` will only show mail for those two domains.
- If you precede the list with an exclamation mark, you will see mail that goes to domains *not* in the list. For example, entering `!example.com, example.net` shows mail that goes to domains *other thatn* example.com and example.net.

All of the reports can be viewed as HTML tables or exported as CSV or YAML. If your PHP version includes the GD extension, all of the reports include charts (either pie charts or bar charts.)

7.1.1 Classification Reports

The available classification reports are:

1. **Classification of Recent Mail**—a breakdown of recently-received e-mail by type.

2. **Top Mail Relays**—a breakdown of the top sending SMTP relays. You can elect to see all relays, only relays that have sent accepted e-mail, or only relays that have sent rejected e-mail.

3. **Top Spam Recipients**—a breakdown of the top recipients of spam.

4. **Top Viruses**—the most popular viruses received. You can organize the reports by the top virus names, or by the top SMTP relays that have sent viruses.

Figure 7.2 is a sample Top Viruses report:

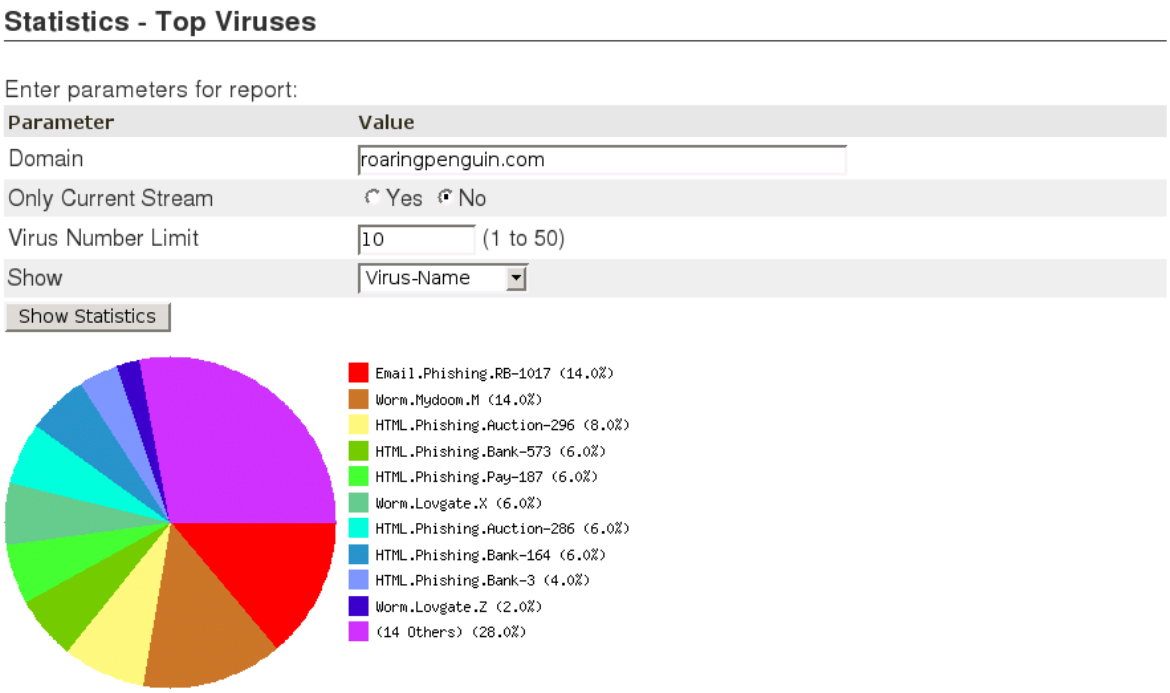
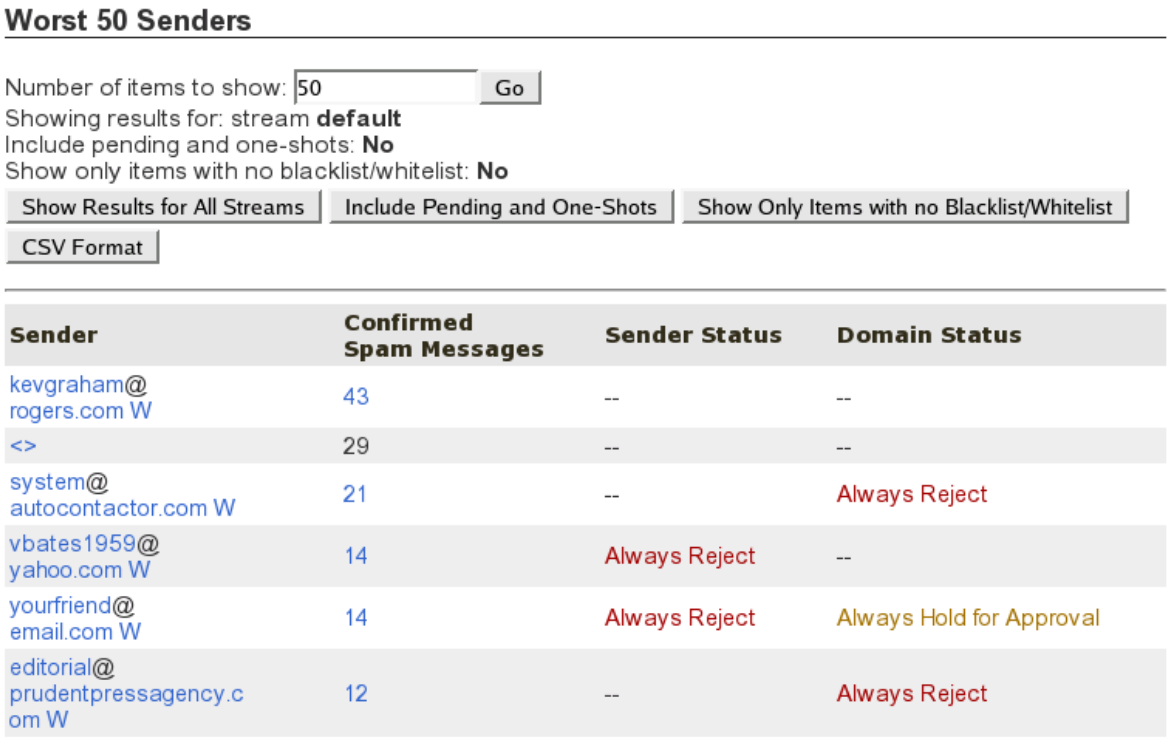


Figure 7.2: Virus Statistics

7.2 Reports based on Trap Content

The "Senders", "Hosts", "Domains" and "Countries" reports are based on the *current* spam trap contents. To select a report, click on **Senders**, **Hosts**, **Domains** or **Countries**. The Sender Report is shown below:



Worst 50 Senders

Number of items to show: 50 Go
Showing results for: stream **default**
Include pending and one-shots: **No**
Show only items with no blacklist/whitelist: **No**

Show Results for All Streams | Include Pending and One-Shots | Show Only Items with no Blacklist/Whitelist | CSV Format

Sender	Confirmed Spam Messages	Sender Status	Domain Status
kevgraham@ rogers.com W	43	--	--
<>	29	--	--
system@ autocontactor.com W	21	--	Always Reject
vbates1959@ yahoo.com W	14	Always Reject	--
yourfriend@ email.com W	14	Always Reject	Always Hold for Approval
editorial@ prudentpressagency.com W	12	--	Always Reject

Figure 7.3: Sender Report

The available reports are:

Sender Report – a list of the top 50 senders of confirmed spam.

Host Report – a list of the top 50 SMTP relays which transmitted confirmed spam.

Domain Report – a list of the top 50 sender domains for confirmed spam.

Country Report – a list of the top 50 sender countries for confirmed spam.

Note that all of these reports base their statistics on the current trap contents.

Normally, these reports only take into account messages explicitly marked as spam. You can have them count pending messages too by clicking on **Include Pending**.

If you wish only to see items that haven't already been blacklisted or whitelisted, click on **Show Only Items with no Blacklist/Whitelist**.

You can obtain reports in CSV format (suitable for importing into a spreadsheet) by clicking on **CSV Format**

Normally, reports are shown only for the current stream. You can get a report for all streams on the system by clicking on **Show Results for All Streams**.

7.3 Greylisting Report

The greylisting report (available only to administrators) is useful only if you have enabled "Tempfail unknown senders on first transmission". It obtains its data from the table that records retransmission attempts. The main greylisting report shows you the worst domain-names used by senders of greylisted messages. You can click on a domain name to see details about greylisted messages (supposedly) from that domain.

7.4 Load Report

Note: This section describes features that only the CanIt-PRO System Administrator can use.

The Load Report shows the load on your CanIt-PRO system. To access the report, click on **Reports** and then **Load**. Select which hosts you wish to monitor, which measurements you wish to see, and the timeframe to display. Click **Show Load** to display the load. A typical display is shown in Figure 7.4.

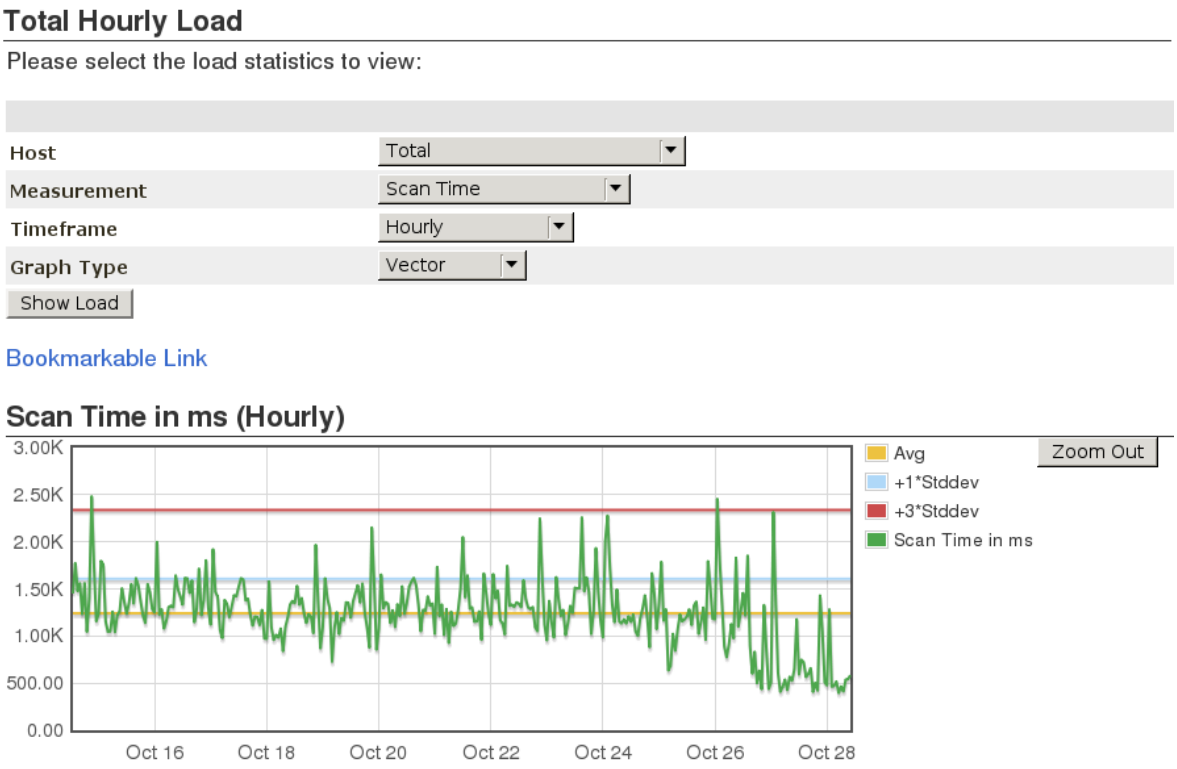


Figure 7.4: Cluster Load

To display a load report:

1. Select the host whose statistics you wish to display. Select "Total" to display totals (or averages

for scan and RCPT times) for all hosts in the cluster. Select "All" to display graphs for all hosts in each chart.

2. Select the measurement to display. Possibilities are:

   - **Average Busy Scanners**: The average number of busy scanning processes at any given instant.
   - **Scan Time**: The time (in milliseconds) to scan an e-mail.
   - **Scans per Second**: The number of messages scanned per second.
   - **RCPT Time**: The time (in milliseconds) to process each SMTP RCPT command.
   - **RCPTs per Second**: The number of RCPT commands per second
   - **All**: Display all measurements.

3. Select the time frame of the report. You can select "Minute-by-Minute", "Hourly" or "Daily". If you select "Daily", you may also select the number of days to show, and the end date of the graph.

4. Select the graph type: "Vector" uses the HTML Canvas element to display the graphs. You can zoom in by drawing a rectangular zoom area with the left mouse button. Zoom out by clicking on **Zoom Out**.

   If the "Vector" format does not work (typically, if you are using Internet Explorer rather than Firefox), choose the "PNG Images" graph type, which produces non-zoomable PNG image output.

On Vector graphs that plot either a single host or the total across the cluster, up to three additional lines may be present:

- The **Avg** line shows the average value of the data.
- The **+1*Stddev** line shows the average plus one standard-deviation.
- The **+3*Stddev** line shows the average plus three standard-deviations.

Chapter 8

Streams

In CanIt-PRO, all of your mail goes into a particular *stream*, and that stream holds all of your rules, blacklists, whitelists and so on.

You may have access to one stream, or to more than one stream. This chapter shows you how to change the settings on your mail stream, and to access other streams.

8.1 Opting Out of Spam Scanning

Each stream can individually opt in or out of spam scanning. If a stream is opted out of spam scanning, then all mail for that stream is passed unchanged. In addition, blacklist rules are ignored. *Hovever, virus-scanning is not skipped; messages can still be held or rejected if they contain viruses.*

To opt in or out of spam scanning, click on **Preferences** and then **Opt In/Out**. Then click on the button to toggle between opting-in and opting-out. Remember that opting in or out is done on a per-stream basis, not on a per-user basis.

8.2 Stream Settings

Each stream can have its own settings relating to certain spam-handling options. To edit stream settings, click on **Preferences** and then **Stream Settings**. The Stream Settings page (Figure 8.1) appears. Remember, every setting on this page applies to only one particular stream; each stream can have its own settings.

Stream settings can be inherited. If you click on **Show Setting Inheritance**, CanIt-PRO will put a little tag near the setting ID showing where the setting comes from. This tag will either be “Global” (meaning the setting is inherited from global settings) or the name of a stream.

The “ID” column is a unique identifier for each setting; it is not used except as a convenient way for Roaring Penguin support personnel to indicate a particular setting over the phone.

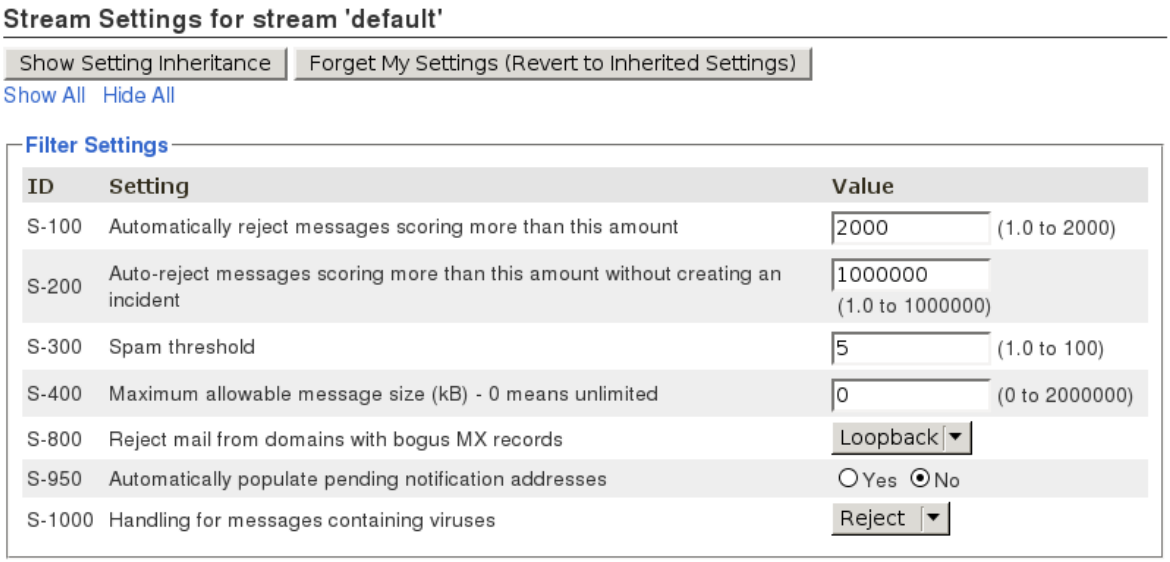


Figure 8.1: Stream Settings

The available settings are:

S-100 Automatically reject messages scoring more than this amount If a message scores higher than this on the spam scale, it will be automatically rejected.

S-200 Auto-reject messages scoring more than this amount without creating an incident If a message scores higher than this setting, CanIt-PRO rejects it *and does not create an incident.* There is therefore no way to search the trap for such messages. Be sure to set this score high enough that the chances of a false positive are extremely remote. On very busy mail servers, rejecting obvious spam without creating an incident can reduce the load on the database server.

S-300 Spam threshold CanIt-PRO will hold any messages scoring higher than this amount. The default value of 5 has been carefully tuned to minimize errors. You should not change it lightly.

S-400 Maximum allowable message size (kB) - 0 means unlimited If non-zero, specified the maximum message size that will be accepted for the stream. Note that any global setting of `MaxMessageSize` in the Sendmail configuration file will still apply. As a safety measure, CanIt-PRO will not reject messages smaller than 100kB, regardless of the value of this setting.

S-800 Reject mail from domains with bogus MX records This setting can take one of three values:

- **No** – do not test sender domains for bogus MX records.
- **Loopback** (the default) – reject mail from any domain that has an MX record in the 127.0.0.0/8 network.
- **All-Bogus** – reject mail from any domain that has an MX record in any of the following networks: 10.0.0.0/8, 127.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 169.254.0.0/16, 224.0.0.0/4, 240.0.0.0/5, 0.0.0.0/32 and 255.255.255.255/32.

S-950 Automatically populate pending notification addresses Stream owners can asked to be notified of pending mail. One piece of information CanIt-PRO requires is the e-mail address to be notified. If you set S-950 to **Yes**, then CanIt-PRO will automatically set a stream's notification address the first time an e-mail passes through the stream.

S-1000 Handling for messages containing viruses If you have a supported virus scanner, you can set this to **Accept** to accept messages containing recognized viruses, **Hold** to hold them for approval, or **Reject** to automatically reject them. The default setting is **Hold**; we do not recommend using **Accept**.

S-700 Only accept mail for accounts in the Valid Recipients table If this is set to **Yes**, then CanIt-PRO refuses to accept mail for recipients unless they are listed in the Valid Recipients Table (see Section 5.14 on page 52.)

S-710 Maximum number of entries in Valid Recipients table If this is set to non-zero, then CanIt-PRO will limit how many entries can be created in the Valid Recipients Table. This is useful for providers who wish to impose such a limit; you can set this setting and then remove the permission for stream owners to modify it.

S-750 Copy all mail in this stream to this e-mail address If you enter an e-mail address for this setting, CanIt-PRO will "Bcc" all mail passing through the stream to the address you specify.

Note: Some countries have laws regulating the copying or redirection of mail. For example, in Canada, Bill C-28 (2010), section 7, prohibits the altering of destination addresses without the express consent of the sender or recipient. Before you use this feature, make sure you are in compliance with the law.

S-900 Hold mail from any sender not listed in Senders Table If this is set to **Yes** then CanIt-PRO will hold messages from any sender that doesn't have a sender rule (such as **Always allow** or **Always reject**. For full details on this feature, please see Section 5.1.1 on page 35.

S-1200 Only tag spam – do not hold any messages If you set this to **Yes**, then *no messages are held in the trap because of high spam scores*. CanIt-PRO simply tags the subject line of each message which would have been held with the string "`[SPAM:***]`" and delivers it normally. The number of stars after the SPAM: tag is the integer part of the spam score.

Be aware that in tag-only mode, CanIt-PRO will still hold messages because of viruses, bad filename extensions and disallowed MIME types. CanIt-PRO will not hold messages because of sender, network or domain "Hold" rules, but any "Reject" rules will still apply.

S-1400 String to put in tagged subjects This is the string that gets prepended to the subject line in tag-only mode if the message is spam. The default setting is `[Spam:%* %?]`. The following special sequences of characters may be used:

- `%*` is replaced with a string of asterisks, where the length of the string equals the integer part of the spam score.
- `%?` is replaced with the reason a message was tagged, such as **SpamScore**, **HoldSender**, etc.
- `%d` is replaced with the actual spam score as a decimal number (e.g. 13.6)

- `%h` is replaced with the actual spam score as a four-digit integer with leading zeros (e.g. 0013)
- `%p` is replaced with the Bayes probability (a real number from 0 to 1.)
- `%%` is replaced with a percent sign.

In addition to the tagged subject, there is a mail header that is added to the message in tag-only mode if it is spam. See Subsection A.1.3 on page 105 for details.

S-1500 String to put in subjects of approved messages If you enter something for this setting, CanIt-PRO will add it to the start of the message subject for every message that was trapped and subsequently released by a person.

S-1600 Tempfail unknown senders on first transmission If you set this to **Yes**, then CanIt-PRO will turn on *greylisting*. This is an effective and cheap way to detect many kinds of spam-sending software, but it may introduce delivery delays the very first time a previously-unknown sender tries to send you e-mail.

S-1620 Minimum delay in minutes before accepting retry from unknown senders If you set S-1600 to **Yes**, we recommend setting S-1620 to between 0 and 2.

S-1700 Permit use of auto-whitelisting If this is set to **No**, then no senders will ever be auto-whitelisted for this stream, even if the system administrator has set up a known-network with auto-whitelisting.

S-1750 Number of days before auto-whitelists expire Auto-whitelists created by CanIt-PRO eventually expire; setting S-1750 controls how long the expiry time is.

S-2100 Plain-text boilerplate to append to messages Any text you enter into this box will be appended to all plain-text e-mails for the stream.

S-2200 HTML boilerplate to append to messages Any text you enter into this box (which should be valid HTML code) will be appended to all HTML e-mails for the stream. If you enter text in the plain-text box, but leave the HTML box empty, then CanIt-PRO uses the plain-text data, surrounded by `<pre>` and `</pre>` tags, for HTML messages.

The remaining stream settings are related to Bayesian analysis and are described in Chapter 9.

8.3 Notification of Pending Messages

CanIt-PRO can send out e-mails periodically reminding you to that you have pending messages in your trap. To turn on notifications, click on **Preferences : Notification**. The Notification Page appears:

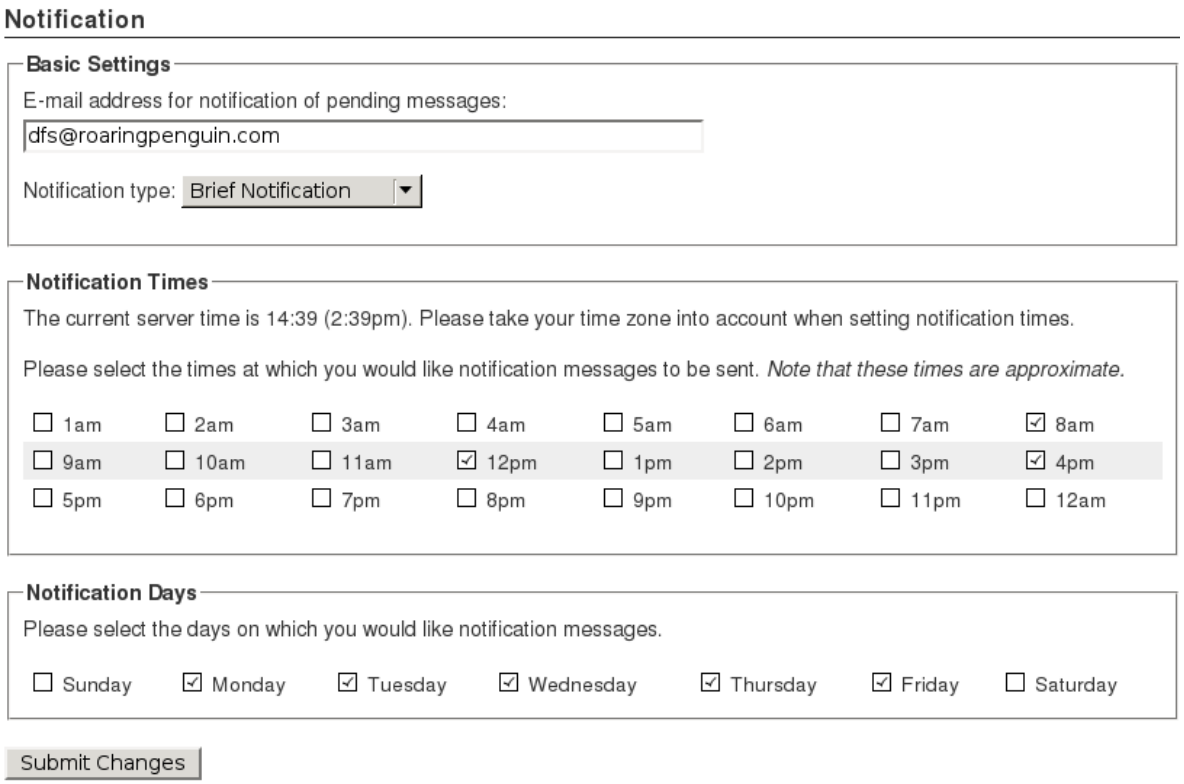

Notification
Basic Settings
E-mail address for notification of pending messages:
dfs@roaringpenguin.com
Notification type: Brief Notification
Notification Times
The current server time is 14:39 (2:39pm). Please take your time zone into account when setting notification times.
Please select the times at which you would like notification messages to be sent. Note that these times are approximate.
1am 2am 3am 4am 5am 6am 7am 8am
9am 10am 11am 12pm 1pm 2pm 3pm 4pm
5pm 6pm 7pm 8pm 9pm 10pm 11pm 12am
Notification Days
Please select the days on which you would like notification messages.
Sunday Monday Tuesday Wednesday Thursday Friday Saturday
Submit Changes

Figure 8.2: Notification Page

To enable notifications:

- Enter the e-mail address to which notifications should be sent. Note that CanIt-PRO attempts to guess the notification e-mail address, but it might guess incorrectly. If CanIt-PRO displays an incorrect notification address, simply erase it and enter the correct address.
- Select the type of notification message:
  1. **Brief Notification** will send short messages that simply inform you that you have pending messages in the trap.
  2. **Detailed Notification** will send longer messages that include sender and subject details for the first 40 pending messages.
  3. **HTML with Links** will send HTML email messages that let you accept or reject incidents directly from within your email reader without having to log into CanIt-PRO. *If you select **HTML with Links**, then anyone who receives the notification will be able to accept or reject the incidents mentioned in the notification email.* You should therefore only select **HTML with Links** if your mail is not automatically forwarded outside of your control.
  4. **Clickable Webform** is similar to **HTML with Links**, but includes additional form elements for accepting or rejecting large groups of messages at once. Note that email reader

support for HTML forms is spotty. Therefore, **Clickable Webform** *may not work* with your email program and you may have to fall back to **HTML with Links**.

- Select the times at which you would like notifications to be sent. You can choose to be reminded as often as hourly. A more practical choice might be three times daily: Once at 8:00am, once at noon, and once at 4:00pm. If you do not wish to receive notifications, simply turn off all of the time checkboxes.

  Be aware that the notification times are approximate. Mail can be delayed for many reasons; you should not expect to receive notifications promptly on the hour.

- Select the days on which you would like notifications. In Figure 8.2, for example, notifications are disabled on Saturday and Sunday.

- Click **Submit Changes** to make your settings take effect.

8.4 RSS Feeds

CanIt-PRO permits you to set up an RSS feed to view your pending messages. To enable an RSS feed, click on **Preferences** and then **RSS Feed**. The RSS Feed Page appears:

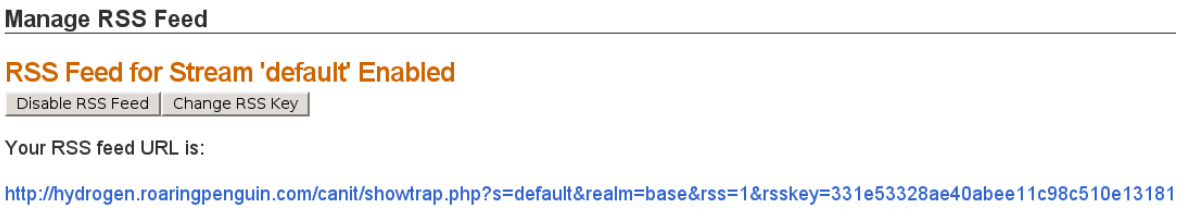


Figure 8.3: RSS Feed Page

To enable the RSS feed, click on **Enable RSS Feed**. An RSS feed URL will be generated; this is the feed location that you put into your RSS reader. The random-looking **rsskey** parameter is what authenticates you to CanIt-PRO.

Note: The RSS feed URL is sensitive! Anyone who obtains the URL can read your Pending Messages RSS feed. You should therefore keep the URL confidential.

If you think your RSS feed has been compromised, you can take one of two actions:

1. You can disable the RSS feed completely by clicking **Disable RSS Feed**.
2. You can create a different key by clicking **Change RSS Key**. This will create a new URL; the old one will no longer work. You will need to update your RSS feed readers with the new URL.

Figure 8.4 shows how the pending messages feed might look in a typical RSS feed reader. Many feed readers allow you to accept or reject the incident directly from within the reader without logging in to CanIt-PRO. To see the incident details, however, you'll need to log in to CanIt-PRO.

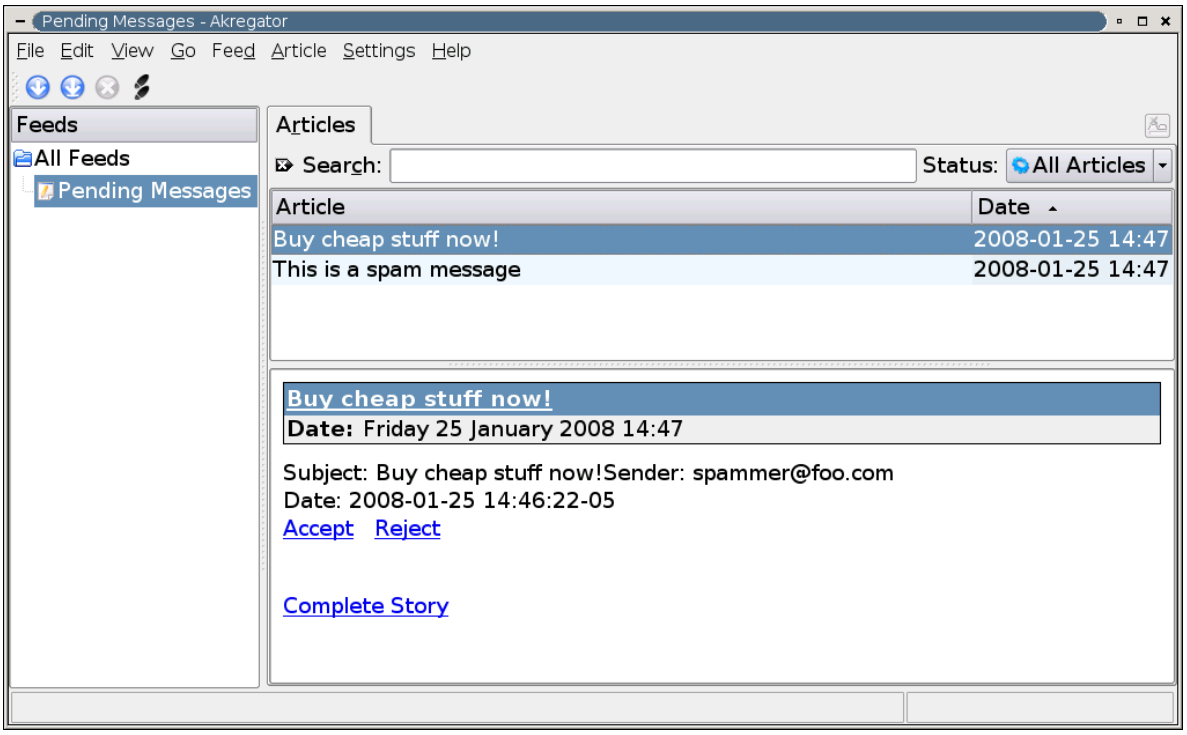


Figure 8.4: Example Feed Reader

8.5 Adding Alternate Addresses

Normally, the CanIt-PRO administrator takes care of making sure all of your mail goes into the correct stream. However, if you have aliases or additional e-mail addresses, you can request those addresses to be added to your stream. In this way, all e-mail for the additional addresses also passes through your scanning rules and spam trap.

Note: Obviously, you can only add e-mail addresses whose mail is normally delivered through the CanIt-PRO server. Although CanIt-PRO will let you add addresses such as `hotmail.com` or `gmail.com` addresses, mail for those streams won't be scanned by CanIt-PRO, because they are outside CanIt-PRO's control.

To add an alternate address to your stream:

1. Click on **Preferences** and then **Alternate Addresses**
2. Enter the e-mail address you want added to your stream. Include only the actual e-mail address (for example, `dfs@roaringpenguin.com`) and not your full name or any comments.
3. Re-enter the address to verify it.
4. Click **Add Address**. CanIt-PRO will compose an e-mail and send it to the address you entered in steps 2 and 3.

5. When the e-mail arrives, click on the link it contains to confirm the addition of the address. Once you have confirmed the addition, CanIt-PRO will route all mail for the address through your stream.

8.6 Switching Streams

A normal user has a selection box of streams she is allowed to switch to, whereas the CanIt-PRO administrator has a text box into which he can type the name of any stream.

To switch streams, pick the name of the stream and click **View This Stream.**

To make the current stream your default stream every time you log in, click **Preferences** and then **Set Default Stream**. The following page appears:

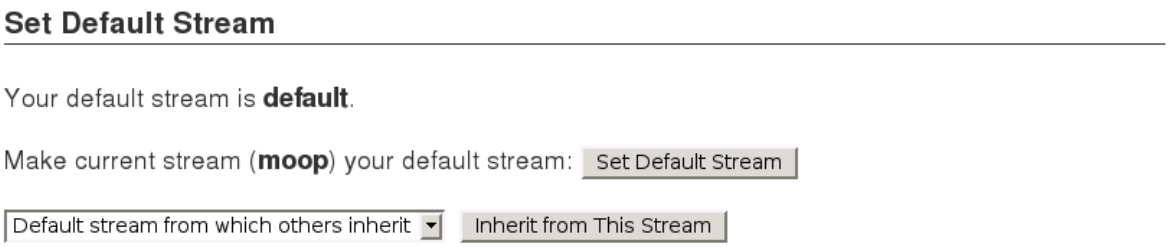

Set Default Stream
Your default stream is default.
Make current stream (moop) your default stream:
Set Default Stream
Default stream from which others inherit
Inherit from This Stream

Figure 8.5: Set Default Stream

A normal user has a selection box of streams she is allowed to switch to,

If you click **Make current stream your default stream**, then the current stream (the one printed near the top of the page) will become your default stream. Each time you log on to CanIt-PRO, you will be logged in to that stream. (This option is only available to users in CanIt-PRO's user table. It is not available to users who authenticate using an external authentication method.)

The second option, **Inherit from This Stream**, lets you select a stream from which to inherit rules and settings. Normally, a stream inherits from the **default** stream, but the administrator may have set up additional streams from which you can inherit. Alternatively, you can choose not to inherit from any other stream.

8.6.1 Viewing All Streams at Once

The CanIt-PRO administrator can enter a special stream, "$\star$" (a single asterisk) in the Switch Stream box. This is not a real stream; rather, it makes it possible to view all trapped messages, rules, blacklists, whitelists, etc. in every stream. The displays are adjusted to include an extra **Stream** column so you can see which stream contains a particular message, rule or blacklist entry. The entries in the **Stream** colums are links which switch to the appropriate stream when clicked.

Chapter 9

Bayesian Filtering

9.1 Introduction to Bayesian Filtering

Bayesian filtering is a statistical technique whereby CanIt-PRO assigns a *spam probability* based on training from users. Bayesian filtering can greatly improve the accuracy of CanIt-PRO, and makes it harder for spammers to evade filtering.

In CanIt-PRO, Bayesian filtering works as follows:

1. Each incoming e-mail message is broken up into *tokens*. Roughly speaking, a token corresponds to a word. In addition to single-word tokens, CanIt-PRO keeps track of *token pairs*, which can greatly increase the accuracy of Bayesian filtering.
2. End users *train* CanIt-PRO by marking a message as spam or non-spam. Each time a message is marked, CanIt-PRO updates counters for each token and token pair in the message. The training statistics are unique for each stream; each stream therefore has its own training set and own notion of what is and isn't spam. The set of messages on which CanIt-PRO is trained is called the *training corpus*.
3. When size of the training corpus is large enough (see the Global Settings list below), CanIt-PRO applies statistical analysis to incoming messages. Each token in the message is looked up to see how many times it appeared in a spam message, and how many times in a non-spam message. The 15 "most interesting" tokens are collected, and a combined probability is computed based on the individual token probability. A token is considered "interesting" if it is either very likely to appear in a spam message, or very likely to appear in a non-spam message. Tokens that can appear in both spam and non-spam messages are not considered interesting.
4. After CanIt-PRO computes the combined probability, it consults a table to add points to (or subtract points from) the spam score.

9.2 Stream Settings Associated with Bayesian Filtering

The following stream settings (under **Preferences : Stream Settings**) affect the Bayesian filter.

S-2300 Enable Bayesian analysis If you set this to **Yes**, then CanIt-PRO's Bayesian Analysis module is enabled.

S-2310 Enable Bayesian training If you set this to **No**, then although CanIt-PRO performs Bayesian Analysis, it does not permit you to train its Bayesian analyser. Enabling Bayesian analysis but disabling Bayesian training might make sense if you only want to inherit training from another stream.

S-2400 Inherit Bayes training history from these streams This is a per-stream setting that allows one stream to share other streams' Bayesian history. For example, if there is a stream that has particularly good Bayes training, you can enter its name in this setting to inherit its training. In general, you can use a comma-separated list of stream names, and all of their training will be inherited.

If your administrator is using the Roaring Penguin Training Network (RPTN) to share Bayes data, you should enter `@@RPTN` in this box.

S-2500 Add links to messages to train Bayesian analyzer This setting can be **No**, **Inline**, **Separate-Part** or **Plain-Separate-Part**. If you select **No**, then CanIt-PRO does nothing special with messages that pass through it. If you select **Inline**, then CanIt-PRO adds hyperlinks to the end of the message. Clicking one of the hyperlinks trains CanIt-PRO's Bayesian analysis engine, allowing you to mark a message as spam even if it is not caught in the trap. **Separate-Part** is similar, except the training links are stored in a separate HTML part rather than placed in the original message text. Finally, **Plain-Separate-Part** adds a separate plain-text part with the voting links. Some mail readers misbehave if there is a plain-text message followed by an HTML part—they render the HTML part as the message. Microsoft Outlook, in particular, seems to suffer from this deficiency, so Outlook users may want to choose **Plain-Separate-Part**.

S-2600 Add training links to messages even if whitelisted Normally, CanIt-PRO adds Bayesian training links to all scanned messages. If you do not want to add training links to messages from whitelisted senders, set this setting to **No**.

S-2700 Add training links in message headers If you set this to **Yes**, then CanIt-PRO will add three special headers containing training links to the message. These headers will be named `X-Antispam-Training-Spam`, `X-Antispam-Training-Nonspam`, and `X-Antispam-Training-Forget`. These permit the training of a message as spam or non-spam, or to forget training, as indicated in the header name. This can be a less-obtrusive way to add training links to messages, and it won't break PGP/MIME messages. However, users need to know how to view full message headers to use the training headers.

S-2800 Remove pre-existing Bayesian training links from incoming mail If an incoming piece of mail has CanIt-PRO training links in it, they should probably be removed because they are likely to either originate from a different CanIt-PRO installation, or have been forwarded inadvertantly. If you relay all your mail through CanIt-PRO, you should set this to **Yes** so links are removed from forwarded or incoming messages.

S-2900 Only train on error when spam corpus reaches this size Once your spam history reaches a certain size, it may be worthwhile only to train CanIt-PRO if it misclassifies non-spam as spam. If you change this setting to 200 (for example), then once you have 200 items trained as "spam",

CanIt-PRO only trains on items you *accept* out of the trap display page. You can still explicitly train spam messages from the Incident Details page.

S-3000 Score below which to auto-learn as non-spam If an incoming mail scores below this threshold, CanIt-PRO automatically trains it as non-spam. If you use this setting, you should enable **Add links to messages to train Bayesian analyzer**. This allows you to correct errors if CanIt-PRO misclassifies a piece of mail.

The default setting of -1000 means CanIt-PRO will practically never auto-learn. We do not recommend setting the auto-learn threshold above zero.

S-3100 Score above which to auto-learn as spam If an incoming mail scores above this threshold, CanIt-PRO automatically trains it as spam.

The default setting of 10000 means CanIt-PRO will practically never auto-learn mail as spam. We do not recommend setting this threshold below 10.

S-3200 Permit unauthenticated voting If you set this to **Yes**, then when you click on a training link to vote an e-mail as spam or non-spam, CanIt-PRO will register the vote even if you are not logged in (and without prompting you to log in.) Use this setting with care; if S-3200 is **Yes**, then anyone who receives a copy of your voting link can vote on the message.

9.3 Training the Bayesian Filter

Each time you accept or reject a message, CanIt-PRO's Bayesian filter is trained on that message. It is therefore easy to build up a body of trained spam messages.

Because many more messages in the trap are rejected rather than accepted, it takes longer to build up a body of trained non-spam messages. For that reason, you should enable **Add links to messages to train Bayesian analyzer** and train the system on non-spam messages until a suitable body has been built up. You train the system simply by clicking on the appropriate training link.

If you click on a training link, you'll be taken to the Voting screen:

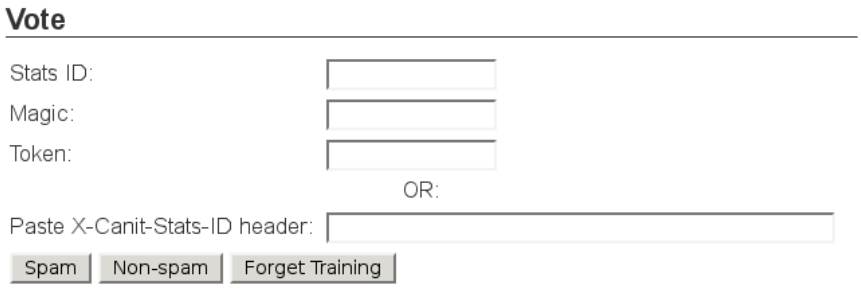


Figure 9.1: Bayes Voting Screen

The screen will reflect the results of your vote by saying that the message was marked as spam or non-spam.

9.3.1 Manual Voting

If you do not have Bayesian training links, you can "manually" train the Bayes engine as follows:

1. In your mail reader, view *all* of the message headers. The way you do this depends on the software you use to read mail.
2. Look for a header that looks like this:

   `X-Canit-Stats-ID: number - hex_string`

   The *number* is a decimal number, and the *hex_string* is a string of numbers and letters. The *number* is the Stats ID, and the *hex_string* is the "Magic" value.

   If the header has three parts like this:

   `X-Canit-Stats-ID: number1 - hex_string - number2`

   Then *number1* is the Stats ID, *hex_string* is the "Magic" value, and *number2* is the "Token". The token is a date in the form *YYYYMMDD*.
3. Click on **Rules** and then **Vote**.
4. Enter the Stats ID and the Magic value in the appropriate entry boxes. If there is a token, enter it in the **Token:** box. Otherwise, leave the token box empty.

   NOTE: Instead of entering the Stats ID, Magic and Token values separately, you can simply copy the entire X-Canit-Stats-ID: header into the **Paste X-Canit-Stats-ID header** box to save time.
5. Click on **Spam**, **Non-spam** or **Forget** to train the Bayes engine appropriately.

9.4 Bayesian Score Settings

To configure the scoring mechanism for Bayesian filtering, click on **Rules** and then **Bayes Settings**. The Bayes Settings screen appears:

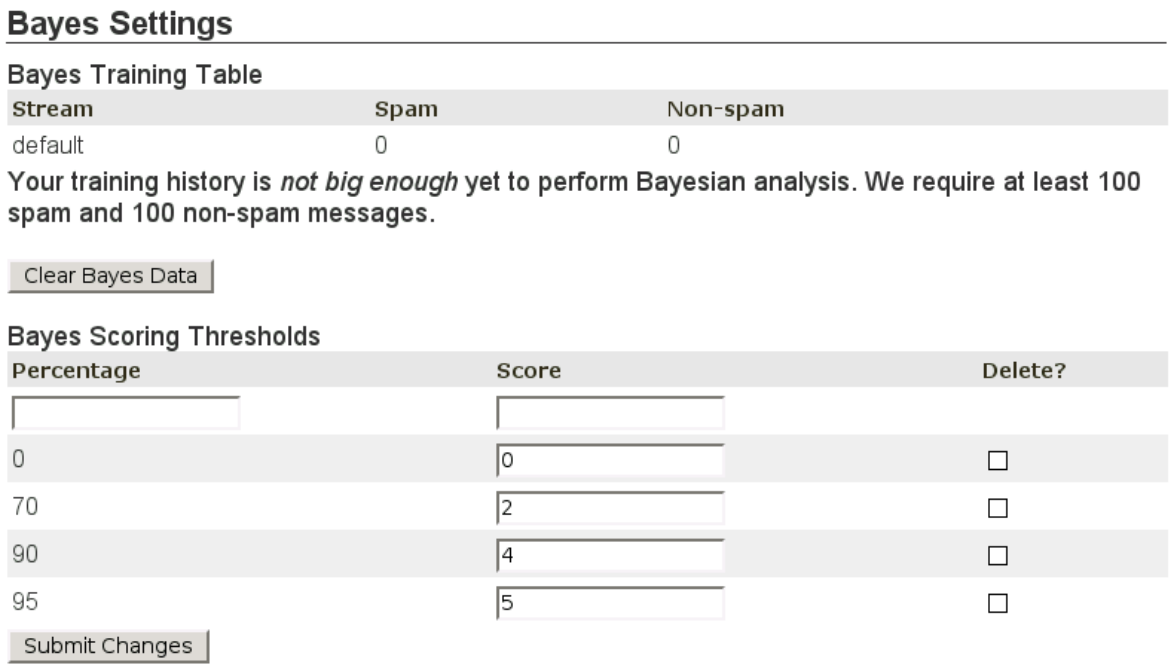


Figure 9.2: Bayes Settings

The training history table shows the current state of the Bayes database:

- **Spam** indicates the number of spam messages in the training database.
- **Non-spam** indicates the number of non-spam messages in the training database.

To configure Bayesian settings, enter a set of percentage and scores into the table. CanIt-PRO determines the score as follows:

- CanIt-PRO calculates the *spam probability*. This is a number from 0 to 1. It then multiplies by 100 to convert the probability to a percentage from 0 to 100.
- CanIt-PRO consults the Bayes Settings table to find the largest entry less than or equal to the actual percentage. It then uses the score associated with that entry.

  In the example, the table has entries for percentages 0, 70, 90 and 95. Incidents with a spam probability of 0 to just less than 70 percent do not adjust the score. Probabilities from 70 to just less than 90 percent add 2 to the score. Probabilities from 90 to just less than 95 percent add 4 to the score, and probabilities of 95 percent or more add 5 points to the score.

  In our experience, it is dangerous to subtract points for e-mail with a low Bayesian score. Some spam is caught by the heuristics, but would be missed by Bayesian scoring. If you do choose to use negative scores for low probabilityes, we recommend a small negative score (around -0.5).

If you wish to clear your training set, click on **Clear Bayes Data**. This *deletes all of your traning corpus*. CanIt-PRO will no longer use Bayesian filtering until your training corpus reaches a sufficient size once again.

Chapter 10

Email Archiving

10.1 Introduction to Archiving

CanIt-PRO has an optional add-on component that archives all email that actually gets delivered. That is, CanIt-PRO does not archive rejected mail or messages that expire out of the pending trap, but it does archive everything else.

Note: Archiving is an extra-cost add-on and may not be available in your installation of CanIt-PRO. If you would like to purchase archiving, please contact your sales representative. See the CanIt-PRO Installation Guide for details about installing the archiver.

10.2 Configuring Archiving

Archiving may be enabled or disabled on a per-stream basis. To enable or disable archiving, click on **Archived Mail** and then **Configure**. The Archive Configuration Screen appears:

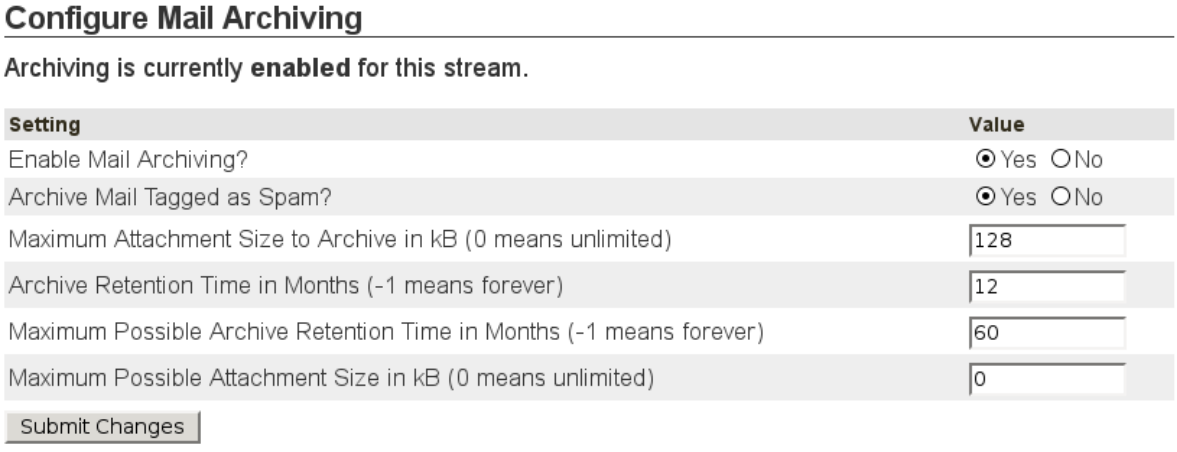


Figure 10.1: Archive Configuration Screen

1. If you wish to enable mail archiving for the stream, set "Enable mail archiving?" to **Yes**. Otherwise, set it to **No**.

2. Normally, CanIt-PRO archives all mail that it delivers, even if the mail was tagged as spam (for those users running in tag-only mode.) If you do not wish to archive tagged mail, set "Archive Mail Tagged as Spam?" to **No**. Please note that disabling archiving of tagged mail *may* cause some legitimate mail not to be archived. (Sometimes, legitimate mail is inappropriately tagged.)

3. Normally, CanIt-PRO does not archive non-text attachments larger than 128kB. Instead, it replaces them with a note explaining that a large attachment was removed. The note details the original attachment name, MIME type and size. You can increase the size limit by adjusting "Maximum Attachment Size to Archive in kB". Setting this value to 0 causes CanIt-PRO to archive *all* attachments, regardless of how big they are. (If you enter a number larger than 0 but smaller than 128, CanIt-PRO automatically rounds it up to 128.)

4. If you are the administrator, you can select how long to retain mail for. Enter an integer in the "Retain archived messages for this many months" box to specify how long to retain messages. A value of -1 means archived messages will *never* be deleted. Any non-negative number less than 1 is automatically rounded up to 1 and any number higher than 1 is accepted as is.

Note: Only the administrator can set the archive retention time.

5. Click **Submit Changes** to update the settings.

10.3 Archiving Outbound Mail

If mail is forced into a stream by a Known Networks entry, it is assumed to be outbound mail. In this case, CanIt-PRO archives the mail in the *sender*'s stream rather than the forced-to stream. In this case, the sender's stream settings are used to determine whether or not to archive the message and for how long to retain it.

10.4 Archiving Internal Mail

Normally, CanIt-PRO does not even see internal mail because it stays on your internal mail server without passing through CanIt-PRO. However, there is a hook for archiving internal mail. To archive internal mail, perform the following steps. (Only the CanIt-PRO administrator has permission to perform them.)

1. Click on **Archived Mail** and then **Authorized Hosts**

2. Enter the IP address of your internal mail server *as seen by CanIt-PRO* in the "IP Address" box.

3. Click **Submit Changes**

4. Configure your internal mail server to copy all internal mail to the address **x-archive-robot@*host***, where *host* is the fully-qualified host name of your CanIt-PRO machine. If you have a cluster of machines, use the host name of the least-loaded scanner.

Note: Details for configuring your mail server to copy internal mail to an external address are beyond the scope of this document. Consult your mail server vendor for assistance.

Note: Make sure to configure your mail server to copy *only* internal mail to the x-archive-robot address. You can also copy mail from internal users to external users *providing* your external mail does not go out via CanIt-PRO. If CanIt-PRO is copied on messages that it has already seen, it will reject them

When CanIt-PRO archives internal mail, it relies on the From:, To:, Cc: and Bcc: headers to determine where to archive mail. CanIt-PRO always archives mail in the stream corresponding to the From: email address. It also archives mail in streams corresponding to all To:, Cc: and Bcc: addresses *that are in the same domain as the From: address*.

10.5 Searching the Archives

To search the archives, click on **Archived Mail** and then **Search**. The Archive Search Page appears:

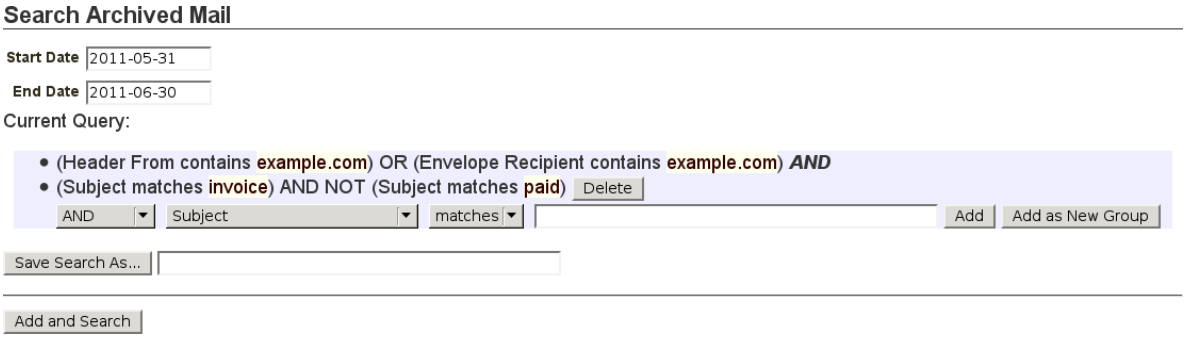


Figure 10.2: Archive Search Page

(Figure 10.2 shows the page with a search query built. Initially, the search query will be empty.)

The Archive Search Page permits you to build up a complex search query and then execute it. Here's how search queries work:

- A query is a list of zero or more *groups*. Each group is evaluated as a unit before evaluating the next group.
- Each group consists of one or more *expressions*. Each expression is evaluated as a unit.
- An expression consists of a *field*, a *relation* and some *data*. These will all be explained soon.

- Within a group, expressions are joined with AND, OR, AND NOT or OR NOT. The AND operator is evaluated with higher precedence than OR. (If you include NOT, the NOT negates the next expression.) Thus, for example, a query like:

  ```
  (X = 1) AND (Y = 2) OR (A = 3) AND NOT (B = 4)
  ```

  is evaluated as:

  ```
  ((X = 1) AND (Y = 2)) OR ((A = 3) AND (NOT (B = 4)))
  ```

- Within a query, groups are joined with AND, OR, AND NOT or OR NOT. Again, the AND operators have higher precedence than OR.

10.5.1 Fields

The possible fields for searching the message archive are:

- **Subject** — The message subject.
- **Body** — The full text of the message body (plain-text and HTML parts only.)
- **Envelope Sender** — The SMTP envelope sender email address.
- **Header From** — the email address in the From: header.
- **Envelope Recipient** — The SMTP envelope recipient addresses.
- **Attachment Filename** — The file names of any attachments.
- **Stream** — The stream name.

The following additional fields are available, but are less generally useful than the basic fields outlined above:

- **Incident ID** — The CanIt-PRO Incident ID, if any.
- **Client HELO** — The HELO string submitted by the SMTP client.
- **Previous-Hop Relay Address** — The IP address of the machine that connected to CanIt-PRO to send the message.
- **Previous-Hop Relay Hostname** — The host name of the machine that connected to CanIt-PRO to send the message.
- **Actual Relay Address** — The IP address of the machine that sent the message, possible parsed from the Received: headers.

- **Actual Relay Hostname** — The host name of the machine that sent the message, possible parsed from the Received: headers.
- **Message-ID** — The Message-Id: header value.
- **References** — The References: header values.
- **Queue-ID** — The Sendmail Queue-ID.
- **Archive Host** — The hostname of the CanIt-PRO machine that archived the message.
- **Size** — The size of the message in bytes.

10.5.2 Relations

The following relations are available for comparing fields to data. All relations that compare strings are *case-insensitive*. That is, "EXAMPLE" and "example" are considered the same.

Note that not all fields permit all relations; CanIt-PRO automatically restricts the relation pulldown based on the field name. The relations are:

- **matches** — Perform a full-text match.
- **is** — The field must exactly match the data.
- **contains** — The field must contain the data as a substring.
- $>$ — The field must be lexically or numerically greater than the data.
- $<$ — The field must be lexically or numerically less than the data.
- $>=$ — The field must be lexically or numerically greater than or equal to the data.
- $<=$ — The field must be lexically or numerically less than or equal to the data.

The relations permitted by the various fields are:

- **Subject** and **Body**: Only **matches**.
- **Envelope Recipient**, **Attachment Filename** and **References**: Only **is** and **contains**.
- All other fields permit all possible relations except for **matches**.

10.5.3 Creating a Query Expression

To create a query expression, follow these steps:

1. Select a field from the pull-down list of fields.
2. Select a relation from the pull-down list of relations.

3. Enter the data to match against in the entry box.
4. If you already have a partial query built, select one of AND, OR, AND NOT or OR NOT from the pulldown. That operator will be used to join the new expression onto the end of the current expression. The NOT variants negate the sense of the new expression. (That is, NOT converts "is" to "is not", "contains" to "does not contain", etc.)
5. Click **Add** to add the expression to the current query.

If you make a mistake, you can delete the most recently created expression by clicking **Delete**.

10.5.4 Creating a Query Group

To create a new query group, follow the same steps as for creating an expression, but click on **Add as New Group** instead of **Add**. This makes the new expression the start of a new group; the new group is joined to the previous group with AND, OR, AND NOT or OR NOT as selected in the operator pulldown.

10.5.5 Performing a Search

When your query is complete, click **Add and Search** to actually perform the query. (If you have entered data into the text entry box, that data's expression is added to the query before the search is performed. If the text entry box is blank, the query is used without any additional expression.)

10.5.6 Query Cookbook

This section shows some examples of how to build queries.

All Mail to or from a Domain

Suppose you with to see all mail to or from the domain **`example.org`**. You would want to search for messages where the sender *or* the recipient contains **`@example.org`**. Here's how to build the query:

1. Click on **Archived Mail** : **Search** to start a new query.
2. Select "Header From" from the field pulldown and "contains" from the relation pulldown.
3. Enter **`@example.org`** in the text box.
4. Click **Add**.
5. Change the operator pulldown from AND to OR.
6. Select "Envelope Recipient" from the field pulldown and "contains" from the relation pulldown.
7. Enter **`@example.org`** in the text box.

8. Click **Add**.

The query is now complete. Click **Add and Search** to search.

All Mail to or from a Domain that Contains a Given Word

Now suppose you want to see all mail to or from the domain **`example.org`** that also contains the word "Invoice" in the subject or body. Here's how to build that query:

1. Follow steps 1 through 8 in the previous example.
2. Change the operator pulldown to AND.
3. Select "Subject" from the field pulldown and "matches" from the relation pulldown.
4. Enter **`Invoice`** in the text box.
5. Click **Add as New Group**.
6. Change the operator pulldown to OR.
7. Select "Body" from the field pulldown and "matches" from the relation pulldown.
8. Enter **`Invoice`** in the text box.
9. Click **Add**.

Your query now looks something like this:

- Header From contains @example.org OR Envelope Recipient contains @example.org AND
- Subject matches Invoice OR Body matches Invoice

Because groups are treated as a unit, the query is evaluated as:

```
(Header From contains @example.org OR Envelope Recipient contains @example.org) AND
(Subject matches Invoice           OR Body matches Invoice)
```

Although the query builder does not support the most general form of query, all AND and OR combinations (no matter how complex) can be reduced to a form the query builder can understand (you can construct queries in *disjunctive normal form* and *conjunctive normal form*). See http://en.wikipedia.org/wiki/Disjunctive_normal_form for details.

10.6 Saved Searches

CanIt-PRO permits you to save a search for future use. This lets you create a complex search query once and reuse it many times.

To save a search query, simply create the query under **Archived Mail** : Search. Once you are happy with the query, enter a name in the "Save Search As..." box and click **Save Search As...**.

To view your saved searches, click **Archived Mail** and then **Saved Searches**. The Saved Archive Searches page appears:

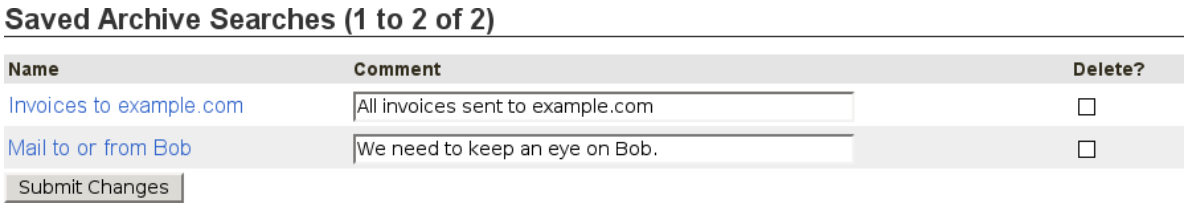


Figure 10.3: Saved Archive Searches

To use a saved search, click on the name of the search. You will be taken to the Archive Search Page with the query pre-created from the saved search. You may use the query as-is or modify it as you wish.

To add a comment to a saved search, fill in the **Comment** box and click **Submit Changes**.

To delete a saved search, enable the appropriate checkbox and click **Submit Changes**.

10.7 Viewing Archived Messages

To view a message from the search results screen, click on the message subject. The message will be displayed in your browser. From within the message display page, you have a number of options:

- Click on **All Headers** to display all of the message headers. By default, CanIt-PRO displays only a subset of the headers.
- Click on **Download Message** to download the original mail message. The message is served up as a **`message/rfc822`** MIME type.
- If an HTML message references external images, CanIt-PRO normally blocks them, replacing them with a stock image that notifies you that external images are blocked. If you wish to load external images anyway, click on **Show External Images**. This link is found at the bottom of the message display.
- If a message has attachments, they are displayed in a list after the message body. Click on an attachment name to download the attachment.

10.7.1 Redelivering Archived Messages

To have CanIt-PRO redeliver a message out of the archive, click on **Redeliver Message** while viewing the message. The Archive Redelivery page appears:

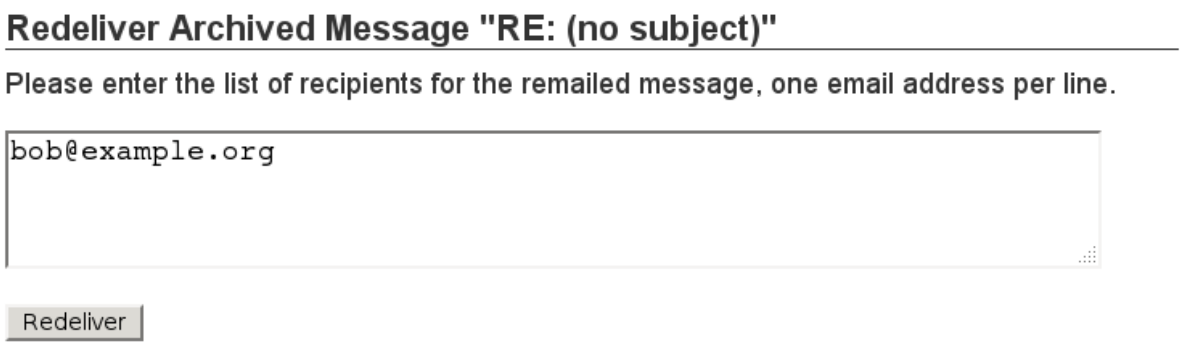

Redeliver Archived Message "RE: (no subject)"
Please enter the list of recipients for the remailed message, one email address per line.
bob@example.org
Redeliver

Figure 10.4: Archive Redelivery Page

By default, CanIt-PRO offers to redeliver the archived messages to the original recipients of the message. However, you can edit the text in the text box to have CanIt-PRO deliver the message to any email addresses you choose.

To queue the message for delivery, click **Redeliver**. Note that CanIt-PRO may take several minutes to actually deliver the message since redelivery runs as a periodic background job.

10.8 Searching for Related Messages

Within the message display page, click on the link **Related Messages** to search for related messages. Given a target message, other messages are considered related to the target if one of these conditions holds:

- The other message's Message-ID appears in the target message's **References:** header.
- The target message's Message-ID appears in the other message's **References:** header.

In most cases, the **Related Messages** link will pull up all the messages in a given thread, allowing you to follow the history of a conversation.

10.9 Seeing Access History

CanIt-PRO records all accesses to archived mail. If you are viewing an archived message, click on **(Access History)** to see all accesses for that message. You can also search the entire access history by clicking **Archived Mail** and then **See Access History**. Enter query parameters to narrow down which accesses you are interested in and then click **Submit**.

10.10 Seeing Search History

CanIt-PRO records all archive searches. To see the search history, click **Archived Mail** and then **See Search History**. Enter query parameters to narrow down which searches you are interested in and then click **Submit**.

Chapter 11

Locked Addresses

11.1 Introduction to Locked Addresses

Locked Addresses are designed to solve the following problem: You want to give out your e-mail address to someone, but you don't trust that person or organization not to turn around and give or sell it to others. You want an address that can only be used by the person or organization you give it to, and not by anyone else.

CanIt-PRO has a complete solution to this problem. However, it does require some administrative overhead before users can take advantage of the feature. If your administrator has not done the setup, then Locked Addresses will not be available for you.

11.2 How Locked Addresses Work

When you create a locked address, CanIt-PRO generates a new random e-mail address, and associates it with your *real* e-mail address. The newly-generated address is in an *unlocked* state. Any e-mail arriving for that address will be delivered to your real e-mail address.

The very first time e-mail arrives for the new address, it locks on to either the sender address or the domain. From now on, only that specific sender (or senders in that specific domain) can send mail to the locked address. Anyone else who tries to send mail to the locked address will receive a "User unknown" error.

There are two settings that affect how a locked address works:

1. The *lock type* can be one of **Domain**, **Address** or **Unlocked**. In the case of **Domain**, anyone in the same domain as the initial sender can send to the locked address. If the lock type is **Address**, then only the initial sender (and no-one else) can send to the locked address. If the lock type is **Unlocked**, then the address always allows anyone to send to it. This may not seem very useful, but in fact, unlocked addresses are convenient for creating temporary e-mail addresses that are easy to rescind later.

2. The *action if lock violated* setting determines what happens if the lock is violated. (A lock is

said to be "violated" if e-mail for a locked address arrives from someone who is not allowed to send to that address.) There are three options:

(a) **Hold mail in trap** causes the violating e-mail to be held in your trap (regardles of what its spam score would be.) You should use this action if you use a locked address to post to a mailing list, because readers of the mailing list could legitimately try to e-mail you.

(b) **Reject mail** causes the violating e-mail to be rejected with a "User unknown" error. This is the best setting to use if you're giving out an e-mail address to someone you don't quite trust.

(c) **Deactivate address** is just like Reject mail, except it *also* deactivates the locked address so no-one at all can use it. You can use this setting if you really want to punish someone for giving out your e-mail address; if they give it out, then even they can't use it any more.

11.3 Creating a Locked Address

To create a Locked Address:

1. Click on **Rules** and then **Locked Addresses**.
2. Click **Create a New Locked Address**. The Locked Address Creation page appears:

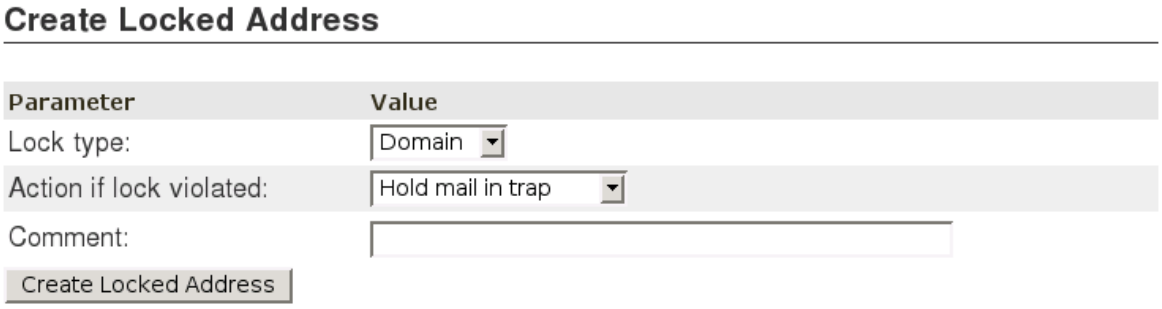


Figure 11.1: Locked Address Creation

3. Select a lock type (one of **Domain**, **Address** or **Unlocked**).
4. Select the action to take if the lock is violated (one of **Hold mail in trap**, **Reject mail** or **Deactivate address**.
5. If you like, enter a comment into the Comment: field to help you remember why you are creating the locked address. For example, if you're creating an address to paste into a Web form, you could put a little note about the Web site in the Comment: field.
6. Click **Create Locked Address**. Your new address is displayed:

Figure 11.2: New Locked Address

You can cut-and-paste the address from the Web page into the Web form or any other window.

11.4 Viewing Locked Addresses

To view locked addresses, click on **Rules** and then **Locked Addresses**. The Locked Address Listing page appears:

Figure 11.3: Locked Address Listing

On the listing page:

- Enable **Delete** and click **Delete Selected Addresses** to delete one or more locked addresses. Deleting a locked address completely removes the address from the system. Note that there is a *very small chance* that CanIt-PRO will generate the same address randomly in the future,

causing confusion. However, the probability of this happening is extremely low, so you don't really need to worry about it. You're far more likely to be hit by lightning than to suffer from a Locked Address collision.

- Click on the name of a locked address to edit it.
- Enter appropriate values in the **Filter Conditions** fields and click **Apply Filter** to restrict which locked addresses are displayed. This lets you search for particular locked addresses. If you've entered meaningful comments when creating locked addresses, it can be very useful to search on the Comment: field.

11.5 Editing a Locked Address

If you click on a Locked Address's name, the Locked Address Editor appears:

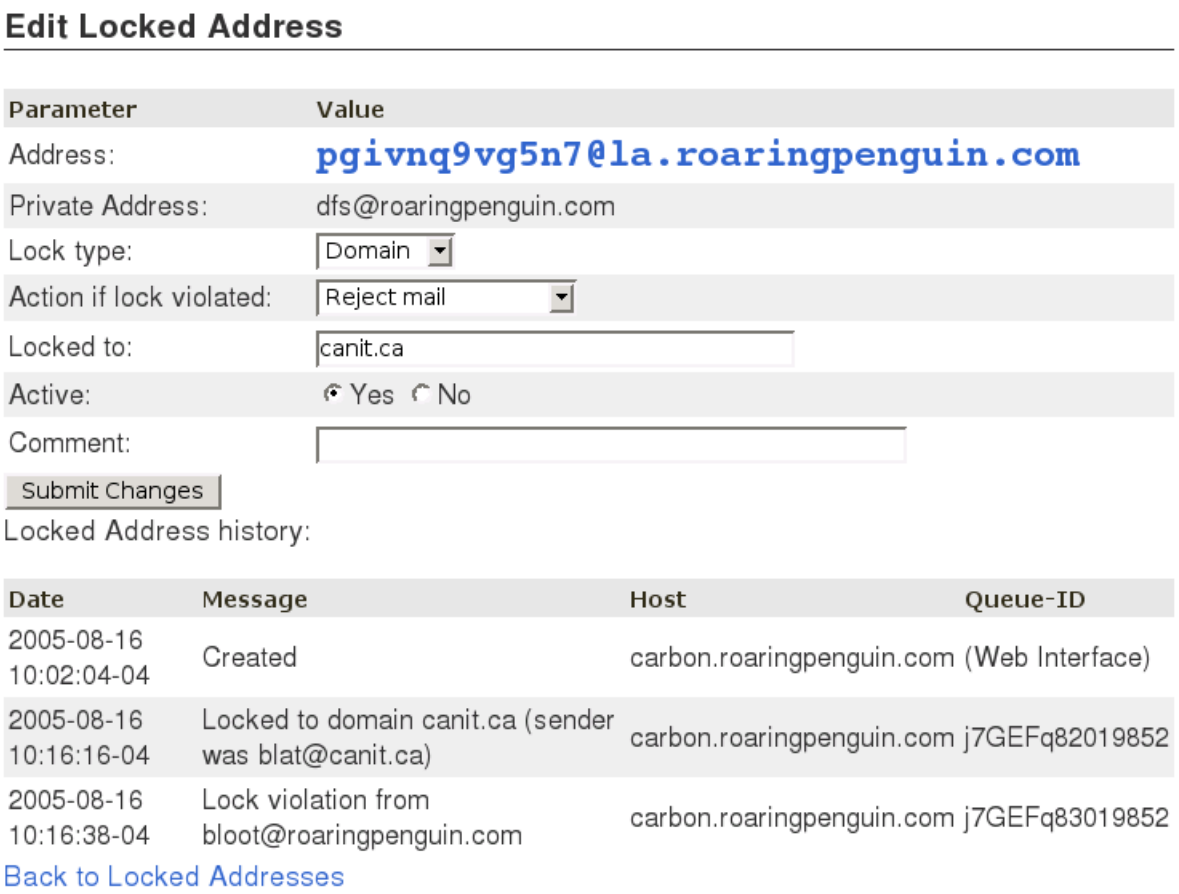


Figure 11.4: Locked Address Editor

In the Locked Address Editor, you can take the following actions:

- Change the lock type by selecting a new value for the **Lock type:** field.

- Change the violation action by selecting a new value for the **Action if lock violated:** field.
- Manually change what the address is locked to by editing the **Locked to:** field. If you make the **Locked to:** field blank, then the address reverts to its pristine unlocked state.
- Activate or deactivate the address by setting the **Active:** field to **Yes** or **No**. If you deactivate a locked address, then any mail sent to it is rejected with a "User unknown" error.
- Change the comment by editing the **Comment:** field.

To make your changes take effect, click on **Submit Changes**.

The bottom part of the Locked Address Editor shows the history of the locked address. In this example, we see the following history:

1. The locked address was created at around 10:02am from the Web interface running on `carbon.roaringpenguin.com`
2. At around 10:16am, mail from `blat@canit.ca` arrived for the locked address, and cause it to lock to the domain `canit.ca`. The mail arrived on the scanning machine `carbon.roaringpenguin.com` and had Sendmail queue-ID j7GEFq82019852. (This last bit of information is useful only for system administrators who might want to correlate events with their mail logs.)
3. A few seconds later, mail from `bloot@roaringpenguin.com` arrived and was rejected because of a lock violation.

11.6 Deciding on a Lock Type and Violation Action

Here are some guidelines for deciding on which lock type to use:

- If you wish to create an address for the purpose of subscribing to a mailing list, *and* you want to allow list members to e-mail you off-list, then select a lock type of **Unlocked**. If you find the address is abused, you can simply deactivate it manually.
- If you wish to create an address for the purpose of subscribing to a mailing list but you prefer not to be e-mailed off-list, select a lock type of **Sender** or **Domain**, and a violation action of **Hold mail in trap**. This causes off-list replies to be held in your trap for review.
- If you wish to create an address for the purpose of obtaining information from one organization (for example, by filling in a Web form), select a lock type of **Domain** and a violation action of **Reject mail** or **Deactivate address**.
- If you wish to create an address that only one person can use (for example, you give out your business card to someone at a conference), select a lock type of **Address** and a violation action of **Reject mail** or **Deactivate address**.

Chapter 12

Tips

Managing spam requires constant attention, but there are many things you can do to reduce your workload. This chapter offers advice for setting your CanIt-PRO settings.

12.1 Don't Trust Sender Addresses

Many spammers use one-time disposable sender addresses. Many addresses are not even valid. So we do not recommend blacklisting addresses unless you receive many different spam addresses from the same address. Therefore:

> Blacklisting individual addresses is usually not effective. Whitelisting known good addresses (for example, mailing-list sending addresses) can be very effective. The sender report may, however, highlight a persistent spam sender address which is worth blacklisting.

12.2 Don't Trust Sender Domains

Just as sender addresses are often fake, sender domains are too. However, some domains are known spammers and these can be profitably blacklisted. The tip:

> Blacklisting entire domains can be effective under limited circumstances. Whitelisting known good addresses (for example, mailing-list sending addresses) can be very effective. Holding all mail from free e-mail services like Hotmail and Yahoo can be effective if you use it in conjunction with whitelisting of known good senders from those services. Use the domain report to help make these decisions.

12.3 You May Trust Relay Hosts

It is rather difficult to fake the IP address of the SMTP relay host, so this attribute can usually be trusted. We recommend using a DNS-based blacklist service in your Sendmail configuration file to

reject the most obvious offenders. However, if you receive multiple spam messages from a given relay host, it can be effective to block the host:

> Blacklisting a repeat-offender relay host is effective. Whitelisting known good hosts such as internal hosts is effective and recommended. Use the host report to determine which hosts are persistent spam relays.

12.4 Custom Rules

12.4.1 General Recommendations

There are a couple of custom rules that are sometimes quite effective:

1. Custom rules which specify Sender contains "offer", "bounce", "return" and "noresponse" can often trap spam. You should use only moderate scores on these rules, because some legitimate mail comes from such senders. However, adding a rule which scores 3 or so for these patterns can help catch a lot of spam which might otherwise sneak under the scoring threshold.
2. Subject-matching rules for the most obnoxious spams are very effective. For example, Subject regexp-match rules against `v\Sagra` and `(increase|enlarge).*penis` are very effective.

12.4.2 Things to avoid

Be very careful when writing custom rules, especially rules that can match on the message body. For example, a straightforward rule that contains "cum" in the body will match mail containing mail containing "document", "cumulative", "modicum" and at least 64 other common English words. Similarly, "sex" will match "sexton", "Essex" and others.

If you want to match words in a message body, we recommend that you use a regular-expression match, and use Perl's word-boundary operators. For example, the Perl regular expression `\bcum\b` matches the word "cum", but not "document", "cumulative" or "modicum".

Never whitelist your own e-mail address or domain. Spammers often fake messages as if they come from their intended victim, precisely because they know that many people whitelist their own address or domain. In fact, as extra protection, CanIt-PRO now ignores whitelists of your own address or domain.

12.5 Group High-Scoring Messages Together

We recommend that you set the default sort order to sort by Score, Descending. This groups high-scoring messages at the beginning and low-scoring messages at the end of the pending list. This makes it easier for you to dispose of the messages.

> Reduce your workload by sorting message summaries by Score, Descending. This lets you use the interface more effectively.

12.6 Roaring Penguin Best-Practices

At Roaring Penguin Software Inc., we've spent quite a bit of time analyzing spam and spammers. You may wish to try out some of our anti-spam rules to see if they work well for you. Here is a quick summary of the rules we use; they may inspire you to develop your own anti-spam rules.

- We use custom rules to add 3 to any message whose **Sender** contains "offer", "noresponse", "remove", "marketing" or "promo". These rules may be a touch aggressive, but we have found them quite effective.
- Another custom rule adds 1.2 to any **Relay** containing "[" (left square bracket.) This indicates a reverse-DNS failure on the sending host, which is mildly correlated with spamming.
- We use a discard threshold of 20; this seems quite safe.

12.7 General Anti-Spam Tips

12.7.1 Use Receive-Only Addresses on your Web Site

Spammers love to extract e-mail addresses from Web sites, and not only do they use them for the obvious purpose of spam targeting, but also they use them as fake sender addresses.

Therefore, we recommend a general policy of publishing only generic e-mail addresses on your Web site, like `info@roaringpenguin.com` and `sales@roaringpenguin.com`. When you reply to inquiries, always use a real, personal e-mail address like `dfs@roaringpenguin.com`. This has two benefits:

1. If someone sends e-mail purporting to come from `info@roaringpenguin.com`, you know immediately that it is spam, and you can reject it. You can blacklist all your generic addresses inside CanIt-PRO.
2. If someone complains about receiving e-mail from one of the generic addresses, you can point to your policy and assure the recipient that the sender address was faked.

12.7.2 Do Not Reply to Spam

Do not ever reply to spam e-mail; such replies simply serve to validate your e-mail address. Similarly, do not visit Web sites purporting to offer opt-out services; they also serve to validate your address for further spamming.

Appendix A

Mail headers added by CanIt-PRO

CanIt-PRO adds several headers to an email message containing details of the filtering tests performed on the message. This chapter lists these headers and describes their contents.

A.1 General Headers

A.1.1 X-Spam-Score

This header contains combined details of all tests performed by CanIt-PRO. It has two general forms. The first is for messages that get fully scanned and scored, and the second is formessages that bypass the standard scoring.

The first form is the most common, and appears as:

```
X-Spam-Score:  5.2 (*****) [Tag at 5.0] HTML_MESSAGE,234(0.5),RBL(spamrbl.example.com,1.0)
```

In this form, the header contains the score as a number, followed by zero or more stars indicating the spamminess in ( ) brackets, and what the nearest hold or tag threshold was, in [ ] brackets.

At the end of the line is a list of tests that were triggered by this message. As of the current release, these are the possible contents of this test list:

- SpamAssassin rule hit (e.g. `HTML_MESSAGE`)

  This shows a SpamAssassin rule hit. They will appear first in the list of tests, and generally consist of all uppercase letters, digits, and underscore (_). The list of possible rules is too long to describe in this document.

- Custom Rule hit (e.g. `234(0.5)`)

  This shows a Custom Rule hit, and takes the form of

  `rule-number(rule-score)`

  The *rule-number* number is unique within a CanIt-PRO installation across all streams, and may identify a rule in the current stream or any of its parents.

- Mismatch Rule hit

This shows a Mismatch Rule hit, and takes the form of

`Mismatch(`*`sender-address`* `mismatches` *`relay-name`*`)`

The *sender-address* is the envelope sender of the message, and *relay-name* is the hostname of the sending SMTP server.

- RBL Scoring hit

  This shows an RBL hit, with score applied. It takes the form of:

  `RBL(`*`rbl-name`*`;`*`rbl-score`*`)`

  The *rbl-name* is the name of the RBL triggered, and *rbl-score* is the score assigned to that RBL by the RBL Rules.

- SPF Rule hit

  This shows an SPF scoring action. It takes the form of:

  `SPF(`*`spf-result`*`;`*`spf-score`*`)`

  The *spf-result* is the result of the SPF query (pass, fail, etc – see Section 5.11 for details), and *spf-score* is the score applied for that result.

- Bayesian analysis score

  This shows the score applied due to Bayesian analysis. This item will only be present if the Bayes engine results in a non-zero score. It takes the form of:

  `Bayes(`*`bayes-probability`*`;`*`bayes-score`*`)`

  This is the same as the content of the **`X-Bayes-Prob`** header, where *bayes-probability* is the probability between 0 and 1, and *bayes-score* the score applied for that probability.

The second form of this header occurs when no scoring is performed. This can occur because of a whitelist entry, a trapped and released message, or because of an error in CanIt. In this form, the `X-Spam-Score` header will contain one of the following:

- `undef - user@example.com is whitelisted`
- `undef - example.com is whitelisted`
- `undef - 192.168.1.1 is whitelisted`

  The above three cases occur when a sender, domain, or host are whitelisted, respectively.

- `5.2 (message approved - incident 12345)`

  This occurs when a message was manually approved from the spam trap, and passed through. The first number is the original score of this message before approval.

- `undef - spam scanning disabled`

  This occurs when spam scanning has been disabled for this stream. In this case, the message was not scanned for spam.

- `undef - message too big (size: 8000000, limit: 1024000)`

  This occurs when the message is larger than the administrator's threshold for scanning spam. The message size and the threshold value are indicated in the header.

- `undef - no license key found`

  This occurs when the product's license key has not been installed, or is expired. In this case, the message was not scanned for spam.

- `undef - Database unavailable, message NOT spam-scanned`

  This occurs when the CanIt-PRO database is not accessible for some reason. This is generally indicative of a problem with the CanIt-PRO installation.

A.1.2 X-CanItPRO-Stream

This header contains the name of the stream, and all streams it inherits from. The general format of this header is:

`X-CanItPRO-Stream: mystream (inherits from otherstream, default)`

where `mystream` is the current stream, and `otherstream` and `default` are streams that `mystream` is inheriting rules and settings from.

A.1.3 Subject

CanIt-PRO may tag the **`Subject:`** header with scoring information. This tag may be customized on a per-stream basis. See "String to put in tagged subjects" in Section 8.2 for details on what this tag may contain.

A.1.4 X-Spam-Flag

This header is added if CanIt-PRO is operating in tag-only mode, and the message scores over the tag threshold. It always appears as

`X-Spam-Flag: YES`

It is used to trigger filtering rules and for compatibility with various email clients and other software that expect this header to be set on suspected spam.

See Subsection 8.2 on page 71 for details regarding tag-only mode.

A.1.5 X-CanIt-ID

This header is added if a message is accepted after being held within the CanIt-PRO database. It takes the form of:

`X-CanIt-ID: incident-id`

where *`incident-id`* is the ID of the incident in the current stream that was accepted to pass this message.

This header may be removed in a future release of the product.

A.2 Bayesian Filtering Headers

If your site administrator has enabled Bayesian filtering, you will see several extra headers.

A.2.1 X-Bayes-Prob

This header contains the probability of the message being spam, as per your Bayesian training. It takes the form of:

```
X-Bayes-Prob:  0.0001 (Score 0, tokens from:  somestream, @@RPTN)
```

The probability is expressed as a value between 0 (not spam) and 1 (certainly spam). The score is the score applied for that probability value. Following the score is a list of the streams whose tokens were used for Bayesian analysis of the message.

See Chapter 9 for full details on Bayesian filtering.

A.2.2 X-Canit-Stats-ID

This header contains the ID of this message's Bayesian signature. The ID values can be used to vote this message as spam or non-spam by entering them into the appropriate page on the web interface, though generally it is simpler and easier to enable training links and vote directly from the body of the message.

The general format of this header is:

```
X-Canit-Stats-ID: 314300 - 31097dbb7b37
```

If the message has already been trained, this information is available in the header, as one of:

```
X-Canit-Stats-ID: 314300 - 31097dbb7b37 (trained as spam)
```

```
X-Canit-Stats-ID: 314300 - 31097dbb7b37 (trained as not-spam)
```

If Bayesian filtering is enabled, but for some reason a signature is not available in the database, this header will appear as

```
X-Canit-Stats-ID: Bayes signature not available
```

A.2.3 X-Antispam-Training-(Spam,Nonspam,Forget)

If Bayesian filtering is enabled, and a signature is available for the message, CanIt-PRO may add three training headers containing a link allowing the message to be voted as spam, voted as non-spam, or to have any existing votes forgotten. These headers will appear similar to:

```
X-Antispam-Training-Spam:  http://example.com/canit/b.php?i=12&m=31097dbb7b37&c=s
```

```
X-Antispam-Training-Nonspam:  http://example.com/canit/b.php?i=12&m=31097dbb7b37&c=n
```

```
X-Antispam-Training-Forget:  http://example.com/canit/b.php?i=12&m=31097dbb7b37&c=f
```

A.3 Geolocation Header

The `X-CanIt-Geo` header contains geolocation information on the sending relay. It consists of a set of *`key=value`* pairs separated by semicolons. For example, it might look like this:

```
X-CanIt-Geo:  ip=64.26.171.99; country=CA; region=ON; city=Ottawa;
```

The possible key/value pairs are summarized below. Not all are always present; sometimes the location of a server cannot be determined precisely.

- `ip=`*`ipaddr`* — this indicates the IP address of the sending server.
- `country=`*`CC`* — this indicates the two-letter country-code of the sending server.
- `region=`*`reg`* — the region (state, province, etc.) in which the sending server is located.
- `city=`*`city_name`* — this indicates the city in which the sending server is located. Not all IP addresses can be resolved to a city, so this key may be absent.
- `latitude=`*`lat`*`; longitude=`*`long`* — the approximate latitude and longitude of the sending server. If no city could be determined, these simply represent the geographical centre of the country and may have no relation to the actual location of the server.
- `postalcode=`*`postcode`* — the postal code in which the sending server is located.
- `areacode=`*`code`* — the North American area code in which the sending server is located.

If no geolocation information is available, the header looks something like this:

```
X-CanIt-Geo:  No geolocation information available for 127.0.0.1
```

Appendix B

The CanIt-PRO License

READ THIS LICENSE CAREFULLY. IT SPECIFIES THE TERMS AND CONDITIONS UNDER WHICH YOU CAN USE CANIT-PRO

This license may be revised from time to time; any given release of CanIt-PRO is licensed under the license version which accompanied that release.

CanIt-PRO is distributed in source code form, but it is not Free Software or Open-Source Software. Some CanIt-PRO components are Free Software or Open-Source, and we detail them below:

The following files may be redistributed according to the licenses listed here. An asterisk (*) in a file name signifies a version number; the actual file will have a number in place of the asterisk.

File	License
src/Archive-Tar-*.tar	Perl License
src/Config-Tiny-*.tar	Perl License
src/DBD-Pg-*.tar	Perl License
src/DBI-*.tar	Perl License
src/Data-ResultSet-*.tar	Perl License
src/Data-UUID-*.tar	Perl License
src/Digest-MD5-*.tar	Perl License
src/Digest-SHA1-*.tar	Perl License
src/File-Spec-*.tar	Perl License
src/File-Temp-*.tar	Perl License
src/HTML-Parser-*.tar	Perl License
src/HTML-Tagset-*.tar	Perl License
src/IO-Zlib-*.tar	Perl License
src/IO-stringy-*.tar	Perl License
src/Log-Syslog-Abstract-*.tar	Perl License
src/MIME-Base64-*.tar	Perl License
src/MIME-tools-*.tar	Perl License
src/Mail-SPF-Query-*.tar	Perl License
src/Mail-SpamAssassin-*.tar	Apache License, Version 2.0
src/MailTools-*.tar	Perl License
src/Module-Pluggable-Tiny-*.tar	Perl License

File	License
src/Net-CIDR-Lite-*.tar	Perl License
src/Net-DNS-*.tar	Perl License
src/Net-IP-*.tar	Perl License
src/Time-HiRes-*.tar	Perl License
src/TimeDate-*.tar	Perl License
src/URI-*.tar	Perl License
src/YAML-Syck-*.tar	Perl License
src/clamav-*.tar	GPLv2
src/libwww-perl-*.tar	Perl License
src/mimedefang-*.tar	GPLv2

ALL REMAINING FILES IN THIS ARCHIVE (referred to as "CanIt-PRO") ARE DISTRIBUTED UNDER THE TERMS OF THE CANIT LICENSE, WHICH FOLLOWS:

THE CANIT LICENSE

1. CanIt-PRO is the property of Roaring Penguin Software Inc. ("Roaring Penguin"). This license gives you the right to use CanIt-PRO, but does not transfer ownership of the intellectual property to you.

2. CanIt-PRO is licensed with a limit on the number of allowable protected domains or mailboxes. This limit is called "the Usage Limit".

   CanIt-PRO usage may be purchased on a yearly basis, or you may purchase a perpetual license.

3. You may use CanIt-PRO up to the Usage Limit you have purchased. If you have purchased yearly usage, you may continue to use CanIt-PRO until your purchased usage time expires, unless you purchase additional time. If you have purchased a perpetual license, you may continue to use CanIt-PRO indefinitely, providing you do not violate this license.

   If you have purchased yearly usage, you may exceed your purchased limit by up to 10% until the yearly renewal date, at which time you must purchase a sufficient limit for the increased number of domains or mailboxes.

   If you have purchased a perpetual license, or wish to increase your usage more than 10% above your paid-up limit, you must purchase the additional usage within 60 days of the increase.

4. You may examine the CanIt-PRO source code for education purposes and to conduct security audits. You may hire third-parties to audit the code providing you first obtain permission from Roaring Penguin. Such permission will generally be granted providing the third-party signs a non-disclosure agreement with Roaring Penguin.

5. You may modify the CanIt-PRO source code for your own internal use, subject to the restrictions in Paragraph 9 below. However, if you do so, you agree that Roaring Penguin is released from any obligation to provide technical support for the modified software. If you wish your modifications to be incorporated into the mainstream CanIt-PRO release, you agree to transfer ownership of your changes to Roaring Penguin.

6. You may make backups of CanIt-PRO as required for the prudent operation of your enterprise.
7. You may not redistribute CanIt-PRO in source or object form, nor may you redistribute modified copies of CanIt-PRO or products derived from CanIt-PRO.
8. If you violate this license, your right to use CanIt-PRO terminates immediately, and you agree to remove CanIt-PRO from all of your servers.
9. Restrictions on modification:
   (a) Notwithstanding Paragraph 5, you may not make changes to CanIt-PRO or your software environment which would allow CanIt-PRO to run without a valid License Key as issued by Roaring Penguin. You also agree not to set back the time on your server to artificially extend the validity of a License Key, or do anything else which would artificially extend the validity of a License Key.
   (b) You may modify the Web-based interface only providing you adhere to the following restrictions:
   (c) At the bottom of every CanIt-PRO web page, the following text shall appear, in a size, color and font which are clearly legible:
   Powered by CanIt-PRO (Version x.y.z) from Roaring Penguin Software Inc.
   where x.y.z is the product version. In addition, "CanIt-PRO" shall be a clearly-marked hypertext link to `http://www.roaringpenguin.com/powered-by-canit.php`
   (d) You may not include elements on the CanIt-PRO Web interface that require plug-ins (such as, but not limited to, Macromedia Flash, RealPlayer, etc.) to function.
   (e) You may not include Java applets on the CanIt-PRO Web interface.
   (f) If you include JavaScript on the Web interface, you shall ensure that the interface functions substantially unimpaired in a browser with JavaScript disabled.
   (g) You shall not include browser-specific elements on the Web interface. You shall ensure that the Web interface functions substantially unimpaired on the latest versions of the following browsers:
      - Internet Explorer for Windows
      - Mozilla for Windows
      - Mozilla for Linux
      - Konqueror for Linux
   (h) You may not include banner ads on the CanIt-PRO Web interface.
10. Restrictions on reselling services:
    Unless you purchased CanIt-PRO as a service provider on the ISP rate plan, you may not use CanIt-PRO to provide spam-scanning services to third parties. You may use CanIt-PRO only for your employees and contractors accounts on your own corporate servers.
11. Disclaimer of Warranty (Virus-Scanning)
    NOTE: ALTHOUGH CANIT-PRO IS DISTRIBUTED WITH CLAM ANTIVIRUS, WE DO NOT MAKE ANY REPRESENTATIONS AS TO ITS EFFECTIVENESS AT STOPPING VIRUSES. ROARING PENGUIN HEREBY DISCLAIMS ALL WARRANTY ON

THE ANTI-VIRUS CODE INCLUDED WITH CANIT-PRO, OR WHICH INTERFACES TO CANIT-PRO. WE ARE NOT RESPONSIBLE FOR ANY VIRUSES THAT MIGHT EVADE A VIRUS-SCANNER INTEGRATED WITH CANIT-PRO.

B.1 THE CANIT DATA LICENSE

Roaring Penguin makes available certain data that are used by CanIt. This license covers the RPTN Bayes data and the Roaring Penguin RBLs. The data are owned by Roaring Penguin and their use is licensed under the following terms:

1. You may update the RPTN data once per day per Roaring Penguin download username. Roaring Penguin reserves the right to cut off downloads if more than one download per day per username is attempted.
2. You may use the RPTN data only in conjunction with your properly-licensed CanIt installation.
3. You may not redistribute the RPTN data.
4. If your support term expires, you lose the right to use RPTN data for any purpose whatsoever.
5. You may make use of the Roaring Penguin RBLs from within CanIt. You may not query them with any other software.
6. You may use the Roaring Penguin RBLs only in conjunction with your properly-licensed CanIt installation.
7. You may not redistribute the Roaring Penguin RBL data.
8. If your support term expires, you lose the right to use the Roaring Penguin RBLs.

Index

abuse complaints, 30
accept message, 23
action, lock violation, 93
Addresses, Locked, 93
advanced query, 27
alternate addresses, 75
archiving, 83
    configuring, 83
    internal mail, 84
    outbound, 84
    related messages, 91
    saved searches, 90
    searching, 85

Bayesian filtering, 77
    score settings, 80
    stream settings, 77
    training, 79
    voting, 80
best practices, 101
blacklist domain, 23
blacklist host, 23
blacklist sender, 23
blacklisting recipients, 51
bulk entry, 38

change history, 56
changing password, 62
closed, 29
complaints, abuse, 30
configuring archiving, 83
custom rule, 42
    fields, 42
    relations, 43

data license, 112
details, incident, 24
discard, silently, 24

DKIM, 50
documentation, online, 18
domain action, 35
domain matching rules, 36

email archiving, 83
exporting rules, 53
extension, 40

file name, 41
filename extension, 40

greylisting, 13
greylisting report, 67

headers, 103
history, incident, 26
hold unlisted senders, 35
HoldDomain, 22
HoldExt, 22
HoldMIME, 22
HoldRBL, 22
HoldRelay, 22
HoldSender, 22
HoldVirus, 22
host action, *see* network action

importing rules, 56
incident
    closed, 29
    details, 24
    history, 26
    hosts, 26
    ID, 25
    open status, 26
    recipients, 26
    reopen, 29
    reopen, no re-delivery, 29
    resolution, 26

score, 25
spam analysis report, 26
specific, 27
status, 25

license, 109
data, 112
load report, 67
lock type, 93
lock violation action, 93
Locked Addresses, 93

message
accept, 23
reject, 23
message body display, 22
messages
related, 91
messages, pending, 21
milter, 13
MIME type, 39
MIMEDefang, 13
mismatch rules, 46
My Filter, 17

network action, 36
notification, 72

online documentation, 18
open status, 26
opt-in, 35
opting out, 69

password, changing, 62
pending messages, 21
pending messages, notification, 72
postmaster, 53
preferences, 59

query, advanced, 27
quick links, 62
quick spam disposal, 24

RBL checks
skip, 37
RBL rules, 45
receive-only addresses, 101
recipient
blacklisting, 51
valid, 52
recipients, 26
reject message, 23
related messages, 91
relay host, 14
reopen, 29
reopen, no re-delivery, 29
report
greylisting, 67
load, 67
reports, 63
resolution, 26
rule
Bayesian, 80
blacklisted recipients, 51
bulk entry, 38
custom, 42
body matching, 45
fields, 42
header matching, 44
relations, 43
DKIM, 50
domain, 35
domain matching, 36
file name, 41
filename extension, 40
importing and exporting, 53
MIME type, 39
mismatch, 46
network, 36
RBL, 45
sender, 33
opt-in, 35
wildcard, 34
SPF, 47
valid recipients, 52

saved searches, 90
score, 25
search trap, 27
searching archived email, 85
sender action, 33
Sender Policy Framework, *see* SPF
show changes, 56

silently discard, 24
Simple Mail Transfer Protocol, *see* SMTP
skip RBL checks, 37
SMTP, 14
spam analysis report, 26
spam disposal, quick, 24
spam trap, 21
    sort order, 22
spam-scanning, opting out, 69
specific incident, 27
SPF, 14, 47
statistics, 63
status, 25
stream, 14
    settings, 69
    switching, 76
    viewing all streams, 76

tag-only mode
    configuring, 71
    X-Spam-Flag header, 105
tempfail, 14
temporary failure, *see* tempfail

valid recipients, 52
VBR, 49
viewing all streams, 76
voting, 80
Vouch by Reference, 49

whitelist domain, 24
whitelist host, 23
whitelist sender, 23
WHOIS queries, 29
wildcard, 34